DISQUISITIONES ARITHMETICAE

CARL F. GAUSS

PRESENTACION.

En 1985 nació la idea, y tendría que pasar una década hasta que ésta se llevara a feliz término. Al igual que habrá sucedido en tantas ocasiones en la comunidad matemática hispanoparlante, nos parecía imperdonable que, ya casi dentro del siglo XXI, no existiera una versión castellana de las *Disquisitiones Arithmeticae* del gran Gauss.

Iniciamos la tarea de realizar esta traducción y si bien no sabíamos cuánto tiempo nos iba a tomar su finalización, sabíamos que tendríamos la mirada puesta sobre nosotros desde que salió en *Historia Mathematica* aquella pequeña notita "A Spanish Edition of *Disquisitiones Arithmeticae*" en 1987. Tampoco era ajena la interrogación permanente de Víctor Albis, que en cada congreso internacional en el que nos juntábamos me espetaba su "¿cómo va la traducción?".

El proyecto nació en la Escuela de Matemática de la Universidad de Costa Rica y contó con el apoyo durante varios años de la Vicerrectoría de Investigación de esta institución. En el desarrollo de este proyecto participaron muchas personas: el profesor Mark Villarino (en un primer momento), los profesores Michael Josephy y Angel Ruiz (durante todo el tiempo) y el profesor Hugo Barrantes (posteriormente). El entonces estudiante de posgrado Alan Dixon ayudó en el uso de TEX para darle su formato. En diferentes formas de respaldo a la elaboración participaron los entonces asistentes Adrián González, Luis Gustavo Hernández, Jesús Peraza y Martin du Saire. Y en la mecanografía nos ayudaron Gastón Guerra, Milton Madriz y Julián Trejos.

Aunque un primer borrador de la obra completa se terminó de hacer en 1988, no fue sino hasta 1990 que completamos una versión definitiva. Y pasaría aún más tiempo hasta que se emprendieran las acciones para buscar su publicación: burocracias usuales en el medio y hasta licencias sabáticas inaplazables conspiraron para atrasar la salida a la luz pública.

La idea de hacer esta traducción no era por supuesto original. Conocemos de otros intentos serios fuera de Costa Rica por hacerla y sabemos también que algunos

avanzaron parcialmente en la tarea y otros, simplemente, no lograron pasar de las intenciones. Aunque haya sido la obra que abrió la teoría moderna de números y que ha sido considerada, con toda justicia, una de las joyas de la producción matemática de todos los tiempos, emprender y completar su traducción no era un objetivo tan fácil de asumir: aparte de la traducción propiamente conceptual, la tarea significaba, inevitablemente, innumerables horas dedicadas a la minuciosa labor de cuidar estilo, simbología usada, representación gráfica, y, además, realizar interminables revisiones para minimizar los errores. La materialización de la idea era lo verdaderamente difícil. Era de entrada un gran reto a la constancia y perseverancia personales.

En la realización efectiva de este proyecto en Costa Rica confluyeron varios factores. El apoyo institucional fue importante. Este se dio a pesar de que, en un principio, se dudaba de la conveniencia ("no era de matemáticas" ni era un proyecto típico de investigación) o de la factibilidad de un proyecto de este tipo que se debía realizar en un plazo de tiempo relativamente largo. Los directores de la Escuela de Matemática durante estos años en algunos casos apenas toleraron nuestro proyecto (porque, tal vez, no les quedaba más remedio), aunque en otros sí lo apoyaron sin reservas. En la Vicerrectoría de Investigación sucedió un tanto parecido, aunque el apoyo dado globalmente fue siempre, sin duda, mucho mayor. Aparte de este apoyo administrativo, fue muy importante también la existencia durante los años ochenta de un ambiente académico propicio para el desarrollo de este tipo de iniciativas. En 1983 se había fundado la *Asociación Costarricense de Historia y Filosofía de la Ciencia* que ha buscado desde su nacimiento fomentar proyectos de investigación, publicación y de reunión académicas en torno a la historia de las ciencias y de las matemáticas en particular. (No sobra indicar que el profesor Michael Josephy ha sido siempre un asociado y colaborador importante de estas iniciativas, que el profesor Hugo Barrantes ha sido durante años el Tesorero de esta Asociación y quien escribe esta presentación ha permanecido como su Presidente desde su fundación). Cabe mencionar, además, que la acción durante estos años de la *Sociedad Latinoamericana de Historia de las Ciencias y la Tecnología* ha permitido importantes intercambios en la comunidad académica latinoamericana preocupada por estos temas, lo que también ha nutrido nuestros esfuerzos. Pero lo que más influencia tuvo fue la persistencia y permanencia de este grupo de matemáticos dispuestos a no cejar en el empeño de obtener la primera versión castellana de las *Disquisitiones*, a pesar de que, como siempre sucede en proyectos de esta dimensión y sobre todo en nuestros países, muchos obstáculos humanos y administrativos se sumaron a las dificultades propiamente intelectuales de la tarea.

El proyecto ayudó a fortalecer los trabajos en la historia y la filosofía de las matemáticas en la Universidad de Costa Rica, los que, recientemente, han encontrado un lugar institucional especial con la creación en 1990 del *Programa de Investigaciones Meta-Matemáticas* (estudios multidisciplinarios sobre las matemáticas y su enseñanza). Varias investigaciones, publicaciones y participaciones en congresos académicos dentro y fuera de Costa Rica fueron nutridas con el trabajo de la traducción.

Ya en lo que se refiere a la traducción propiamente, tratamos de hacerla lo más fiel posible al latín original. Pero consultamos las versiones francesa (trad. A. C. M. Poullet-Delisle, 1807) y alemana (trad. H. Maser, 1889) y sobre todo la versión inglesa de A. A. Clarke (tanto la edición de 1966, como la de 1986 revisada por W. C. Waterhouse). Debe destacarse que en nuestra revisión de la segunda edición inglesa encontramos una colección de erratas que le señalamos directamente a Waterhouse.

Como es lógico suponer, en el desarrollo de nuestra tarea surgieron dificultades filológicas. En cuanto a la semántica, tratamos de hacer una traducción apropiada palabra por palabra, aprovechando que usualmente la palabra latina corresponde a una única palabra castellana, solo en unos casos era necesario modificarla (por ejemplo, el latín "complexus" se traduce como "conjunto" y no como "complejo" aunque el inglés dice "complex"). En cuanto a la sintaxis, la situación era más problemática: a pesar de la similitud de la estructura latina con la castellana fue necesario reordenar muchas veces las frases para obtener la expresión más adecuada en español. Oraciones muy largas en el original latino las tuvimos que dividir. De la misma manera, expresiones latinas muy compactas (como el ablativo absoluto) fueron expandidas. En general, las cláusulas pasivas se tradujeron con la construcción española reflexiva (por ejemplo: "se puede hacer") y evitamos el uso de la primera persona "podemos hacer".

Como nuestro propósito fue hacer una traducción lo más fiel posible al latín, debemos agradecer muchísimo el haber podido contar con la existencia del sistema TEX (versión Macintosh) para el levantamiento del texto y la confección de las artes finales. Con TEX pudimos tratar efectivamente la multitud de símbolos matemáticos, la notación complicada y la enorme cantidad de ecuaciones, buscando siempre una representación gráfica muy parecida a la del original de 1801.

Nos pareció importante incluir en esta versión de las *Disquisitiones* una introducción que permitiera colocar este libro y la obra de Gauss en un contexto apropiado. De igual manera, para beneficio de los lectores, introducimos una lista en lenguaje moderno de los contenidos de cada artículo de las secciones de la obra.

Para terminar esta presentación, y en nombre del equipo que realizó esta primera versión castellana de las *Disquisitiones Artihmeticae*, deseo expresar nuestro agradecimiento a varias personas e instituciones. A la Escuela de Matemática y a la Vicerrectoría de Investigación de la Universidad de Costa Rica. A los colegas, asistentes y amigos que mencionamos hace unos cuantos párrafos y que contribuyeron al éxito de nuestro proyecto. Y, muy especialmente, a la *Academia Colombiana de Ciencias Exactas, Físicas y Naturales* que gentilmente decidió publicar este trabajo y, en particular, a nuestro buen amigo y colega Víctor Albis por su aliento y apoyo constantes.

Angel Ruiz Zúñiga
Presidente
Asociación Costarricense de Historia y Filosofía de la Ciencia
Ciudad Universitaria "Rodrigo Facio"
San José, Costa Rica
28 de mayo de 1995.

INTRODUCCION.

Las ideas que desarrolló Gauss en las *Disquisitiones Arithmeticae*[1] han sido de extraordinaria importancia en la Teoría de Números de los siglos XIX y XX. Gauss realizó una magnífica síntesis de los resultados del pasado en la teoría de números, y obtuvo una colección brillante de nuevos resultados, proposiciones y métodos que han servido desde entonces como escuela para una gran cantidad de los matemáticos más importantes.[2] Se dice, por ejemplo, que el gran Dirichlet siempre tenía una copia de las *Disquisitiones Arithmeticae* en su escritorio, y que estudiaba el libro religiosamente.[3]

Junto con Arquímedes y Newton, Gauss se considera el matemático más grande de todos los tiempos. Y las *Disquisitiones Arithmeticae*, una de las joyas del pensamiento humano.[4]

La vida intelectual de Gauss se desarrolló en un "nuevo" contexto histórico; se trataba de toda una nueva sociedad que emergía de las entrañas de la sociedad feudal. Aunque Gauss vivió parte de su vida en el feudalismo y el absolutismo germanos,

---

[1] Gauss escribió en latín las obras que consideró más trascendentales; el latín de las *Disquisitiones Arithmeticae* fue revisado por el filólogo Meyerhoff; véase Merzbach, U. C. "An Early Version of Gauss's *Disquisitiones Arithmeticae*", en *Mathematical Perspectives*, Academic Press, 1981.

[2] Muchos afirman que con este libro se inicia realmente la Teoría de Números; véase Struik, D. J. *A Concise History of Mathematics*, New York: Dover Publications, 1967; p. 141. (La primera edición es de 1948). Otros estiman que fue Fermat quien creó la Teoría de Números como una ciencia sistemática, pero Gauss inició una nueva fase; cfr. Ore, Oystein: *Number Theory and its History*; New York: Dover Publications, 1948; p. 209.

[3] Cfr. Bühler, W. K. *Gauss: A Biographical Study*, New York: Springer-Verlag, 1981; p. 36.

[4] Las *Disquisitiones Arithmeticae* de Gauss han sido traducidas a varios idiomas: la traducción francesa se tituló *Recherches Arithmétiques* y fue traducida por A. C. M. Poullet-Delisle en 1807; la versión alemana *Untersuchungen über höhere Arithmetik* traducida por H. Maser en 1889; la rusa es de 1959 editada por I. M. Vinogradov, *Trudy po Teorii Cisel*; y la inglesa traducida por A. A. Clarke apareció en 1966, y tiene una versión de 1986 revisada por W. C. Waterhouse.

no puede negarse que la atmósfera de la nueva sociedad afectaba la cultura en su conjunto y, en particular, la producción científica. Esta nueva realidad, que supuso diferentes cosas en la vida de Gauss, y a pesar de que éste nunca salió de su país, le generó interesantes posibilidades para su trabajo y un contacto especial con otros investigadores de las matemáticas. Gauss fue un matemático cuyas contribuciones más que codificar los resultados del pasado abrieron surcos hacia una nueva época. Fue un científico *moderno* en un sentido profundo; su trabajo debe estudiarse por las generaciones de jóvenes como un mecanismo de estímulo para la creación intelectual de todos los tiempos.

Vivió en una época de cambios históricos importantes: cuando Gauss tenía 12 años empezaba la Revolución Francesa, y con ella un cortejo de acciones políticas y militares en el suelo europeo, cuya influencia llega hasta nuestros días.

Nació Johann Friedrich Carl Gauss el 30 de abril de 1777 en la ciudad de Braunschweig (Brunswick).

Ninguno de sus padres poseía una gran cultura y, a lo sumo, sabían leer y escribir.[5] Su familia paterna era de origen campesino.

El talento de Gauss venía de su lado materno. Su madre sostuvo una lucha constante frente a su esposo para que Carl Friedrich pudiera estudiar; tuvo éxito afortunadamente.[6]

Un primer estímulo lo recibió de parte de Friedrich Benz, el hermano de su madre y un hombre altamente inteligente que murió prematuramente.[7] Gauss adoptó como su segundo nombre el de su tío en reconocimiento a ese primer apoyo familiar.

La circunstancia familiar negativa no fue decisiva porque Gauss pudo estudiar la primaria y la secundaria en condiciones relativamente buenas. Como resultaba común en ciudades más o menos importantes de la Alemania de la época, Gauss pudo asistir a la escuela. Su primer maestro fue un tal Büttner; el maestro Büttner—según E. T. Bell[8]—era un bruto al mando de una escuela que esencialmente era una reliquia de la Edad Media.[9] Sabemos que posteriormente Büttner ayudó a Gauss, pero todo pareciera indicar que lo decisivo fue el apoyo del asistente de Büttner,

---

[5] Aunque en el caso de su madre, al parecer no podía escribir.

[6] Cfr. Bell, E. T. : *Men of Mathematics*, New York: Simon and Schuster, 1965 (la primera versión es de 1937); p. 219.

[7] *Idem.*

[8] Cfr. Bell. *Op. cit.* p. 221.

[9] El criterio de Bell difiere del de Bühler, quien tiende a valorar más el estímulo de Büttner para Gauss.

Bartels.[10] Johann Martin Bartels (1769–1836), quien también ejerció cierta influencia en Lobachevsky, hizo conocer las hazañas de precocidad de Gauss, que llegaron a los oídos del Duque de Braunschweig.[11]

Fue en 1791 que Gauss fue presentado al Duque de Brunswick-Wolfenbuttel, quien impresionado por los talentos del joven le concedió un estipendio de diez talentos al año. Cabe decir, que esto no era algo inusual en lugares en Alemania.

Ingresó Gauss al *Collegium Carolinum*, una academia recién creada, con una orientación especial hacia la ciencia; se trataba de una institución pública de muy buena calidad dirigida hacia el personal militar y administrativo del país. Un tipo de institución necesariamente elitista, dentro de un régimen esencialmente absolutista, pero que sirvió para formar a buena parte de los escritores y científicos de la Alemania de la época.[12]

Tal vez resulte interesante comentar que estas academias públicas orientadas a la técnica y a la ciencia encontraban su lugar en el contexto histórico que vivieron los países protestantes; en su lucha contra la Iglesia Católica, los príncipes, acompañados de la Reforma luterana, se dieron a la importante tarea de asegurarse una nueva *intelligentzia*, fuera del control de la Iglesia y capaz de administrar la sociedad de acuerdo a la nueva realidad social y política. Eso explica—en parte—la existencia de instituciones educativas secundarias y universitarias con una vocación hasta cierto punto fundadas y dirigidas por los gobiernos absolutistas de los principados; así como la vocación laica y progresiva de las mismas. La educación y la formación de los cuadros intelectuales fue un componente vital del especial desarrollo de las naciones protestantes en la Europa de la época.

En su ingreso, de nuevo Gauss tuvo ayuda: esta vez de parte de *Hofrath* (consejero) von Zimmermann, quien fuera profesor del *Carolinum*.

De 1792 a 1795 pasó Gauss en el *Carolinum*, siendo este el centro de su vida.

Aprovechó la existencia de una excelente biblioteca; lo que le permitió estar al día en la literatura esencial sobre matemáticas.

Gauss tuvo un interés muy especial por las lenguas y por los estudios clásicos de literatura; de tal manera que cuando a sus 18 años deja el Colegio *Carolinum* aún no se había decidido acerca de su carrera: filología o matemáticas. El asunto lo

---

[10] *Ibid*, p. 223.

[11] Puede consultarse el libro de Edna Kramer: *The Nature and Growth of Modern Mathematics*, Princeton: Princeton University Press, 1981; p. 474. (La primera edición es de Hawthorn Books, 1970).

[12] Cfr. Bühler, *Op. cit.* p. 8.

decidió la construcción del famoso 17-gono el 30 de marzo de 1796: su satisfacción ante el descubrimiento lo convenció de estudiar matemáticas.[13]

Su presencia en la Universidad de Göttingen fue decisiva para su formación intelectual. En esto Gauss no pudo hacer una mejor selección: Göttingen poseía una de las mejores bibliotecas de Alemania y, además, había tenido una reforma decisiva que orientó la universidad hacia la ciencia; más aún, su administración se encontraba menos influida por la Iglesia y por el gobierno. De esta forma, Gauss completó su formación en instituciones que le dieron de lo mejor que se podía conseguir en Europa en cuanto a instrucción, autonomía para el estudio y, además, el apoyo de varias personas para dedicarse a cultivar plena y exclusivamente su espíritu científico. En esto Gauss tuvo una suerte excepcional.

De su experiencia en Göttingen tal vez debamos subrayar que tuvo pocos amigos, entre ellos Bolyai, con quien sostuvo correspondencia toda su vida. Se dedicó enteramente a sus estudios, y lo hizo solo. Este es un dato interesante. Tuvo una intensa experiencia intelectual, solo y sin interrupciones, durante estos tres años; generó durante los mismos buena parte de sus principales ideas científicas, que elaboraría con toda minuciosidad durante el resto de su vida. Es decir, en estos años formuló informal e intuitivamente muchas de sus hipótesis, sus ideas. No es que luego no aparecieran otras ideas o que desechara muchas de las que en estos años formuló, pero que en un tiempo corto generó muchas ideas seminales es un hecho sumamente interesante.[14] Debe recordarse que algo muy similar ocurrió con Newton. En la construcción del conocimiento, la manera en que se producen o generan las ideas es muy variada; a veces se realiza en momentos cortos de gran intensidad que se repiten pocas veces; a veces, en un proceso lento de maduración sistemática coronada con síntesis de creatividad; todo depende de las personas, de su contexto existencial, de su capacidad, etc. Pero un hecho muy importante debe señalarse aquí y es la presencia de la intuición y la opinión, la presencia de lo informal, de las hipótesis que nacen de una percepción intelectual especial, aunque no trascendental o mística

[13] Cfr. Bell, *Op. cit.* pp. 227–228.

[14] El mismo Bell señala: "Para los grandes matemáticos la madurez temprana y una productividad sostenida no son excepción sino la regla. Puede que sea cierto que las ideas más originales se tienen en la juventud; pero cuesta tiempo elaborarlas. Gauss empleó cincuenta años en desarrollar las inspiraciones que tuvo (esta es sustancialmente su propia descripción) antes de que cumpliera veintiún años; e incluso con medio siglo de continuo laborar solo consiguió madurar una pequeña parte de sus ideas". Véase Bell: *Historia de las Matemáticas*, México: Fondo de Cultura Económica, 1985; p. 254. (La primera edición es de 1940 con el título *The Development of Mathematics*, New York, McGraw Hill Book Co.).

sino auténticamente humana. Este componente es esencial en la creación intelectual y en la matemática en particular. Después vendrá la búsqueda de los métodos, las escaleras analíticas, las condiciones formales y las demostraciones precisas, pero esta fase de delinear, de sugerir, de vislumbrar, es esencial en la creación; y, muchas veces, se busca ocultarla por diversas razones, a veces por prejuicio ideológico o por ignorancia. En el caso de Gauss encontramos con precisión un momento de tres años en los que su intuición y creatividad encontraron, como decimos los matemáticos, *un punto de acumulación*.

El principal resultado de Göttingen fue, sin duda, las *Disquisitiones Arithmeticae*.

La teoría de números constituía, según Gauss, la reina de las matemáticas, a la que a su vez consideraba la reina de las ciencias. Y esta no es una mera frase retórica sin trascendencia sino que revelaba una concepción sobre la ciencia y las matemáticas; Gauss utilizaría muchos de los recursos, mecanismos y modelos de la teoría de números en los otros trabajos científicos que realizaría.

Gauss recibió su doctorado de la Universidad de Helmstedt en 1798. Su tesis fue publicada en 1799 con el título: *Demostratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse* (Nuevas demostraciones del teorema que toda función entera racional algebraica en una variable puede ser resuelta en factores reales de primero o segundo grado)[15]; esto será conocido como el "teorema fundamental del algebra". Aunque este resultado ya era conocido[16], incluso con el nombre de Teorema de d'Alembert, Gauss probó que todas las demostraciones anteriores, incluyendo las de d'Alembert (1746), de Euler (1749), de Foncenet (1759) y de Lagrange (1772), eran inadecuadas.[17] En su demostración Gauss transfería sin probarlo la continuidad geométrica a las cantidades aritméticas, pero afirmaba que lo podía demostrar.[18]

---

[15] Cfr. Gauss, C. F., *Werke*, ed. Königliche Gesellschaft für Wissenschften, Göttingen, 12 vols., Leipzig y Berlín, 1863–1950.; III, pp. 3–56.

[16] La primera referencia se encuentra en el trabajo de Albert Girard, editor de los trabajos de Stevin (*Invention nouvelle en algèbre*, 1629). Consúltese el libro de Dirk Struik: *A Concise History of Mathematics*, New York: Dover Publications, 1967; p. 141. (La primera edición es de 1948).

[17] Puede consultarse el excelente libro de Carl Boyer: *A History of Mathematics*, Princeton: Princeton University Press, 1985; p. 548. (La primera edición es de John Wiley & Sons, Inc., en 1968).

[18] Pueden consultarse las líneas fundamentales de este trabajo de Gauss en el libro de Dirk Struik: *A Source Book of Mathematics 1200–1800*, Princeton: Princeton University Press, 1986; pp. 115–123. (La primera edición es de 1969 por Harvard University Press).

La prueba dada por Gauss se basaba en consideraciones de tipo geométrico; sin embargo, en 1816 publicó dos pruebas nuevas, y otra en 1850, buscando una demostración íntegramente algebraica.[19]

Se piensa en nuestros días que este teorema está basado en consideraciones topológicas.

Antes de entrar en las ideas mismas de Gauss, tal vez resulte interesante recapitular algunos elementos de la teoría de números previa a Gauss. Podemos decir que los principales trabajos en la teoría de números anteriores a Gauss fueron realizados esencialmente por Fermat, Euler y Legendre.[20]

Empecemos con Fermat. Hay dos conjeturas de Fermat que tuvieron cada una un destino distinto: a) que los números de la forma $2^{2^n}+1$ eran aparentemente siempre primos, y b) que si p es primo y a es un entero no divisible por p, entonces a^p-1 es divisible por p. Euler demostró en 1732 que $2^{2^5}+1 = 4.294.967.297 = 6.700.417 \cdot 641$. Esta conjetura de Fermat parece no ser cierta para ningún primo mayor que $n = 4$. [21]

Con relación a la segunda conjetura, que es el llamado "teorema menor" de Fermat, fue Euler el primero en publicar una prueba (aunque Leibniz había dejado una demostración en un manuscrito anterior). La prueba de Euler apareció en el *Commentarii* de San Petersburgo en 1736.

En la misma dirección Euler demostró un resultado más general usando la llamada "función de Euler". Se puede probar que

$$\varphi(m) = m(1-\frac{1}{p_1})(1-\frac{1}{p_2})\dots(1-\frac{1}{p_r}) \text{ con } p_1, p_2, \dots p_r \text{ factores primos distintos de } m$$

Euler probó que $a^{\varphi(m)}-1$ es divisible por m si a es primo relativo a m.[22]

Legendre fue un gran matemático francés que hizo aportes a varias partes de las matemáticas y no sólo a la teoría de números. En 1797–98 publicó su libro *Essai sur la théorie des nombres* en dos volúmenes, que constituye el primer tratado dedicado exclusivamente a esta temática.

Legendre redescubrió el teorema de la reciprocidad cuadrática que había sido puesto en términos menos modernos por Euler (aunque su demostración no estuviera

---

[19] Cfr. Boyer, *Op. cit.* p. 549.

[20] Sobre la teoría de números en los siglos XVII y XVIII se puede ver el trabajo del finlandés Raimo Lehti "Gauss's *Disquisitiones Arithmeticae*", *Arkhimedes* **29** (1977), no. 2, pp. 49–66.

[21] Cfr. Boyer, *Op. cit.* p. 499.

[22] *Ibid.* p. 500.

completa). Otro asunto interesante de su trabajo fue que conjeturó en la misma obra mencionada que $\pi(n)$ tiende a $n/(\ln n - 1,08366)$ conforme n crece indefinidamente; no fue sino hasta 1896 que se demostró este resultado: $\pi(n) \rightarrow n/\ln n$ (en el sentido que su razón tiende a 1). Como afirma Bell, muchos de los resultados contenidos en las *Disquisitiones Arithmeticae* fueron obtenidos por ilustres matemáticos anteriores a Gauss, como Fermat, Euler, Lagrange, Legendre y otros. Pero el tratamiento que realizó Gauss fue diferente: aparte de sus propios aportes originales, adoptó métodos generales que permitían englobar la mayoría de los resultados.[23]

Las *Disquisitiones Arithmeticae* fueron publicadas en Leipzig en el verano de 1801, casi tres años después que Gauss había regresado a Brunswick después de su estancia en Göttingen.[24] Se sabe que las primeras cuatro secciones fueron escritas en borrador en 1796 y escritas en forma definitiva para finales de 1797[25] (en este año Gauss envió una copia al consejero Zimmermann, y el levantado de texto se inició en el taller de Kircher); un primer borrador de la Sección Quinta se completó en el verano de 1796, y fue completada a través de diferentes revisiones en el primer semestre de 1800. [26]

Morris Kline señala que las *Disquisitiones Arithmeticae* fueron enviadas primeramente a la Academia Francesa en 1800 y el libro fue rechazado, obligando a Gauss a publicarlo él mismo.[27] Sin embargo, aunque ha sido muy extendida la versión de que las *Disquisitiones Arithmeticae* fueron rechazadas por la Academia Francesa de Ciencias y que ese fue el motivo de que el mismo Gauss asumiera su publicación, todo parece indicar que fue de otra manera. Según Bell, la versión "romántica" es de W. W. R. Ball en su famoso libro de historia de las matemáticas; estudios muy serios en 1935 demuestran que las *Disquisitiones Arithmeticae* nunca fueron sometidas a la Academia Francesa de Ciencias y mucho menos rechazadas.[28]

---

[23] Por ejemplo, el resultado de Fermat que todo primo de la forma $4n + 1$ es la suma de dos cuadrados de manera única, en las *Disquisitiones Arithmeticae* se desprende de la teoría de las formas binarias cuadráticas que Gauss desarrolla. Cfr. Boyer, *Op. cit.* p. 236.

[24] Existen dos manuscritos de una versión preliminar de las *Disquisitiones Arithmeticae*, descubiertos por U. Merzbach; véase "An early version of Gauss's *Disquisitiones Arithmeticae*", *Mathematical Perspectives*, pp. 167–177, Academic Press, New York, 1981. Se describe las diferencias entre las versiones preliminares y las finales.

[25] Véase Bühler, *Op. cit.* p. 18.

[26] *Ibid.* p. 32.

[27] Véase el formidable libro de Morris Kline: *Mathematical Thought. From Ancient to Modern Times*, New York: Oxford University Press, 1990; p. 813. (La primera edición es de 1972).

[28] Cfr. Bell, *Op. cit.* p. 229.

Como es bien conocido, las primeras tres secciones son una recopilación introductoria de los principales resultados de la teoría de números en la época.[29] Las Secciones IV, V y VI son el corazón del trabajo; la Sección VII se refiere a un tema que aunque está ligado en sí mismo constituye una temática aparte.

La primera sección simplemente define la noción de congruencia entre dos enteros racionales módulo p; sólo tiene 5 páginas.

Las Secciones II y III contienen interesantes resultados como la prueba de la unicidad de la factorización de enteros en primos y las definiciones de máximo común divisor, y de mínimo común múltiplo; la investigación de los residuos de una potencia de un número dado módulo un primo, es decir, partiendo del teorema "pequeño" de Fermat: $a^{p-1} \equiv 1 \pmod{p}$, p un primo que no divide a.

El tema central de la Sección IV es la ley de la reciprocidad cuadrática.[30] Aunque ese teorema había sido formulado por Euler, así como discutido por Legendre, Gauss es quien realiza una prueba completa y correcta del teorema.[31]

La Sección V investiga la teoría de las formas binarias cuadráticas, es decir del tipo $f(x, y) = ax^2 + 2bxy + cy^2$ donde a, b y c son enteros dados. El objetivo central en el estudio de estas formas es el de conocer la manera en que un número dado m puede ser representado por las binarias $ax^2 + 2bxy + cy^2$ y las ternarias $ax^2 + 2bxy + cy^2 + 2dxz + 2eyz + fz^2$ [32]; lo cual es esencialmente un resultado aritmético.

Dickson[33] señala correctamente que las binarias así puestas son un caso particular de la fórmula

$$ax^2 + 2bxy + cy^2 = m \qquad (*)$$

que después tendría mucha utilidad en el trabajo de Dedekind, que establece una correspondencia entre clases de formas como en (*) y ciertos conjuntos de números

---

[29] Por lo menos de los resultados disponibles en esas condiciones.

[30] Este ha sido uno de los grandes temas de la teoría de números después de Gauss. Sobre residuos de potencias y reciprocidad, el libro *Reviews in Number Theory*, editado por William LeVeque (Providence, R.I.: AMS, 1974) menciona 81 referencias entre 1940 y 1972, y la continuación del mismo libro, editada por Richard Guy (Providence, R. I.: AMS, 1984), contiene 94 del período 1973–1983.

[31] De hecho, Gauss realizó 8 diferentes pruebas de este teorema en su vida.

[32] Véase Bühler, *Op. cit.* p. 25.

[33] Véase el extraordinario libro del matemático norteamericano Leonard E. Dickson: *History of the Theory of Numbers*, Chelsea, 1951; Tomo III, p. 2. (La primera edición es del Carnegie Institution, 1919–1923, Washington D.C.). Sobre las formas cuadráticas binarias, las cuadráticas ternarias, y las cúbicas, véase las páginas 92–258 de esta obra de Dickson.

algebraicos determinados por una raíz de $a\xi^2 + b\xi + c = 0$. [34]

La Sección VI es un apéndice de la sección anterior; lo que hace Gauss aquí es presentar una colección de aplicaciones de los conceptos que desarrolla en la sección anterior, por ejemplo, para resolver para x e y, la ecuación $mx^2 + ny^2 = A$ con A, m y n enteros.[35]

La Sección VII tuvo una gran influencia; uno de los temas centrales es el de la ciclotomía[36, 37], es decir de la teoría de la división del círculo, referida a la ecuación $x^p - 1 = 0$ con p un número impar. En esta parte se integra una problemática que involucra geometría, aritmética y álgebra de una manera especial: la construcción del polígono regular de n lados con regla y compás.[38] Gauss incluyó su descubrimiento del 17-gono[39], pero además resolvió el problema de manera general, es decir estableciendo cuándo el n-gono se puede construir y cuándo no.[40, 41]

Las *Disquisitiones Arithmeticae* representa también un adiós a las matemáticas puras como campo exclusivo en la actividad científica de Gauss.[42] Aunque, en realidad, no se puede afirmar tajantemente que Gauss se dedicara exclusivamente a la matemática "pura" durante los años de Göttingen.

Tal vez resulte interesante señalar que Gauss tenía prevista la inclusión de una octava sección en las *Disquisitiones Arithmeticae*, pero ésta fue eliminada para bajar los costos de publicación.[43, 44]

---

[34] Para un estudio histórico detallado de las ecuaciones de segundo grado hasta 1920, véase el libro de Dickson, *Op. cit.* pp. 401–428.

[35] Véase Bell, *Op. cit.* p. 236.

[36] Estos cálculos de Gauss anticiparon los métodos generales de Galois treinta años después.

[37] El tema de los polinomios ciclotómicos partirá de este estudio; puede verse un relativamente reciente trabajo sobre esto realizado por el famoso matemático Tom Apostol: "The resultant of the cyclotomic polynomials $F_m(a_x)$ and $F_n(b_x)$", *Math. Comp.* **29** (1975), pp. 1–6.

[38] Véase Bell, *Op. cit.* p. 236.

[39] Un reciente artículo, poco conocido, sobre la construcción del 17-gono regular se puede ver en: Ritseme, N., "Gauss and the cyclotomic equation", *Nieuw Tijdschr. Wisk.* **64** (1976–1977), no. 4, pp. 188–196.

[40] Cfr. Boyer, *Op. cit.* p. 552.

[41] Se puede consultar una introducción sencilla a la construcción de polígonos regulares en el libro de Ore: *Number Theory and its History*; pp. 346–358.

[42] Véase Bell, *Op. cit.* p. 234.

[43] *Idem.*

[44] Se afirma también que durante el período de 1798 y 1800 Gauss introdujo más material en el libro debido a los atrasos en el trabajo editorial, lo que extendió mucho el libro, en particular la Sección quinta.

Parece ser que Gauss tenía la intención de escribir una continuación de las *Disquisitiones Arithmeticae*[45], cuyo contenido podría intuirse a partir de un manuscrito encontrado después de la muerte de Gauss: *"Analysis Residuorum"*, así como de los artículos sobre teoría de números que escribió después de las *Disquisitiones Arithmeticae*. Algunos de los temas habrían sido: el de las sumas, que aparece en el apartado 356 de las *Disquisitiones Arithmeticae*, la teoría de residuos bicuadráticos y cúbicos, y pruebas adicionales de la ley de la reciprocidad cuadrática.

El asunto de las sumas fue desarrollado por Gauss en el artículo *"Summatio quarundam serierum singularium"* de 1808. Se trata de expresiones de la forma

$$W = \sum_{\nu=0}^{n-1} e^{\frac{2\pi i}{n}\nu^2},$$

de importancia en posteriores desarrollos de la teoría de números. Los otros resultados de Gauss sobre residuos bicuadráticos aparecieron en los artículos *"Theoria residuorum biquadraticorum I & II"*, publicados por la Sociedad Real de Göttingen.[46]

Con Morris Kline, podemos decir, en efecto, que las tres principales ideas de las *Disquisitiones Arithmeticae* y de los trabajos de la teoría de números que realizó Gauss son: la teoría de las congruencias, la introducción de los números algebraicos y la teoría de las formas.

La noción de congruencia aparece antes de Gauss con Euler, Legendre y Lagrange; sin embargo, Gauss introdujo la notación moderna en la primera sección de las *Disquisitiones Arithmeticae*:

a es congruente a b módulo p, $a \equiv b \pmod{p}$

b es un residuo de a módulo p, y viceversa.

En la Sección III de las *Disquisitiones Arithmeticae* Gauss analiza los residuos de potencias. En particular, brinda una demostración del teorema "pequeño" de Fermat. Para demostrarlo debe recurrir al estudio de las congruencias del tipo $x^n \equiv a \pmod{m}$; donde a y m son primos relativos.

Es en la Sección IV donde trata el asunto de los residuos cuadráticos; dando aquí su primera prueba de la ley de reciprocidad cuadrática. Aunque Gauss reconoce

[45] Consúltese Bühler, *Op. cit.* p. 29.

[46] *Ibid.* p. 31.

que Euler había estudiado el asunto en su *Opuscula Analytica* de 1783, y que Legendre lo había hecho en su trabajo de 1785, Gauss afirma que eran trabajos incompletos y menos simples que el que presenta en las *Disquisitiones Arithmeticae*.[47]

Gauss realizó en su vida 8 demostraciones[48], y más de cincuenta se han realizado posteriormente.[49]

Gauss estudió la congruencia de polinomios, usando una idea que luego Cauchy usaría para definir los números complejos en *Exercises d' analyse et de physique mathématique*, 4, 1847, 84 ff.[50]

Las leyes de reciprocidad bicuadrática[51] y cúbica fueron trabajadas por Gauss entre 1808 y 1817, y el teorema de los residuos bicuadráticos fue dado en artículos de 1828 y 1832.[52] Sin embargo, señala Bell que es en 1825 que Gauss encuentra que no son los enteros "corrientes" los que le sirven para este asunto, sino los que hoy llamamos "enteros complejos gaussianos" (es decir, de la forma $a + bi$, con a, b enteros racionales). Esto hacía referencia a lo que se desarrollaría como "números algebraicos".[53] Según Kline los enteros complejos ya habían sido introducidos por Euler y Lagrange.[54] Lo que Gauss probó fue que se comportaban más o menos como los enteros racionales ordinarios. En particular, que se cumplía la descomposición única en factores primos para cada entero (asumiendo por supuesto que las cuatro unidades complejas no son diferentes factores: i.e.: si $a = bc = (ib)(-ic)$, no estamos

[47] Véase Kline, *Op. cit.* p. 815.

[48] Para una versión simple de la primera prueba de Gauss de esta ley puede consultarse el artículo de L. Carlitz "A note on Gauss' first proof of the quadratic reciprocity theorem", en *Proc. Amer. Math. Soc.* **11** (1960), pp. 563–565.

[49] Una prueba muy elegante y corta fue hecha por el matemático D. H. Lehmer en el artículo "A low energy proof of the reciprocity law", *Amer. Math. Monthly* **64**, (1957), pp. 103–106. Una prueba algebraica se puede ver en S. Chowla en su artículo "The law of quadratic reciprocity", *Norske Vid. Selsk. Forh.(Trondheim)* **39** (1966), p. 59. Una prueba geométrica en Kaplan, Pierre: "Une demostration géometrique de la loi de réciprocité quadratique", *Proc. Japan Acad.* **45** (1969), pp. 779–780. Véase la de Claës Allander en "Gauss's Law of reciprocity—a transparent proof" en *Nordisk Mat. Tidskr.* **22** (1974), pp. 23–25, 40. Hasta el famoso lógico Th. Skolem no cedió a la tentación de dar una prueba de esta ley, véase "A proof of the quadratic law of reciprocity with proofs of two so-called 'Ergänzunssätze' ", en el *Norske Vid. Selsk. Forh (Trondheim)* **34** (1961), pp. 18–24.

[50] Véase Kline, *Op. cit.* p. 815.

[51] Sobre algunos aspectos de la reciprocidad bicuadrática, véase: Brown, Ezra, "Biquadratic reciprocity laws", *Proc. Amer. Math. Soc.* **37** (1973), pp. 374–376.

[52] Véase Kline *Op. cit.* p. 816.

[53] Cfr. Bell, *Op. cit.* pp. 252–253.

[54] Véase Kline, *Op. cit.* p. 817.

hablando de descomposiciones diferentes).[55] La ley de la reciprocidad cuadrática para enteros complejos fue establecida por Gauss en 1828.[56]

La teoría de los enteros complejos abrió el camino para el desarrollo de una temática apasionante en las matemáticas del siglo XIX: los números algebraicos, aunque el mismo Gauss no percibió la riqueza que este campo supondría.[57] Podemos decir que la teoría evolucionó en cuatro momentos: el primero, su origen, se da con el famoso teorema de Fermat acerca de $x^m + y^m = z^m$. Gauss intentó resolver la conjetura para el caso $m = 7$, pero no tuvo éxito.[58] Gauss no quiso involucrarse mucho con el último teorema de Fermat, en parte por considerarlo una proposición aislada, como muchas otras, que ni puede probarse ni refutarse.[59]

Fue Lamé en 1839 quien lo logró hacer para el caso $m = 7$; y Dirichlet para el caso $m = 14$.

Otro discípulo de Gauss (y de Dirichlet), Kummer, abordó el asunto utilizando una maquinaria teórica que abrió caminos interesantes, e inició la segunda fase en la historia de los enteros algebraicos. Se pasa de los números enteros complejos a los algebraicos, en la formulación de Kummer, los números de la forma

$$f(\alpha) = a_0 + a_1\alpha + \ldots + a_{p-2}\alpha^{p-2}$$

donde α es una p-ésima raíz imaginaria. Kummer llamó a estos números enteros complejos .

Dotados los nuevos números de las definiciones naturales de suma y producto, Kummer asumió la factorización primaria como única, e incluso hizo de esta

---

[55] *Idem.*

[56] Gauss no publicó este resultado; y más bien fue Jacobi, en una serie de conferencias en Königsberg en 1836–1837, quien la estableció; aunque Eisenstein publicó cinco pruebas de la ley desde 1844.

[57] En el tratado de Gauss sobre residuos bicuadráticos, en 1831, Gauss "despejó el misterio que todavía rodeaba a los números complejos a través de su representación por puntos en el plano": Struik. *A Concise* ..., p. 142. Consúltese también el artículo de E. T. Bell "Gauss and the Early Development of Algebraic Numbers", *Nat Math. Mag.*, **18** (1944), pp. 188, 219. Pero debe subrayarse—aún más—que fue Gauss mismo quien dio un tratamiento algebraico y no geométrico a los números complejos, adelantándose seis años a Hamilton (este hecho se descubre en la correspondencia de Gauss con Bolyai en 1837). Véase Bell: *Historia de las matemáticas*, México: Fondo de Cultura Económica, 1985; p. 189. (La primera edición es de 1940 con el título *The Development of Mathematics*, New York, McGraw Hill Book Co.).

[58] *Ibid.*, p. 818.

[59] Cfr. Bell, *Op. cit.* p. 238.

formulación un requerimiento para la resolución de la conjetura de Fermat. (Cauchy y Lamé pensaron como Kummer.) Sin embargo, Dirichlet señaló que eso no era cierto; Kummer reconoció el error muy poco tiempo después. Kummer buscó reconstruir una forma de factorización única a través de unos números que llamó "ideales", logrando la conjetura de Fermat para una serie de números primos: para todos los menores que 100 salvo el 37, 59 y el 67, para los que demostró la conjetura en un artículo de 1857.[60] Posteriormente, Mirimanoff en 1905, perfeccionando el método de Kummer, extendió el resultado para todo n hasta 256 si x, y y z son primos al exponente n.[61]

El asunto de la factorización única se volvió el mecanismo teórico para la definición de nuevos números y entidades.

Otro discípulo de Gauss, Dedekind, avanzó extraordinariamente el campo, definiendo una nueva y decisiva etapa. En lugar de trabajar con las raíces de la unidad, Dedekind, en 1871, formuló una definición más amplia de los números algebraicos: sea r una raíz de la ecuación

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0\,,$$

con los a_i enteros racionales negativos o positivos, y tal que r no es raíz de ninguna ecuación del mismo tipo y de grado menor a n, se llama a r un número algebraico de grado n. Si el coeficiente a_0 es 1, r se llama un entero algebraico de grado n.

Dedekind introdujo el concepto de campo numérico y mostró que claramente los números algebraicos forman un campo; introdujo entonces la noción de anillo, y probó que los enteros algebraicos formaban precisamente un anillo. Con las nuevas definiciones de números ya podía Dedekind buscar una solución al asunto de la factorización única, pero ahora en el campo de los números algebraicos. Para esto sólo le faltaba un nuevo concepto que era precisamente el de ideal, en el sentido moderno. La teoría de los ideales constituye entonces una generalización de los números enteros ordinarios.[62]

Años más tarde, en un trabajo de 1887, Kronecker, discípulo de Kummer, demostró que la teoría de los números algebraicos es independiente de la teoría de los números reales.[63]

---

[60] Véase Kline, *Op. cit.* p. 820.

[61] *Idem.*

[62] *Ibid.* p. 824.

[63] Hilbert en 1897 condensó todos estos resultados y los solidificó en su "Die Theorie der algebraischen Zahlkörper".

La teoría de las formas fue importante en el siglo XIX. Aunque Euler había obtenido algunos resultados, Lagrange descubrió que existían formas equivalentes para expresar un entero. Como ya lo hemos señalado antes, este es el tema central de la Sección V de las *Disquisitiones Arithmeticae*.[64] Gauss probó varios teoremas sobre la equivalencia de las formas. Entre ellos, que dadas tres formas F, F_1 y F_2, entonces: si F es equivalente a F_1 y F_1 es equivalente a F_2, entonces F es equivalente a F_2. Demostró cómo encontrar todas las transformaciones de F en F_1 si F y F_1 son equivalentes, etc. Y, especialmente, encontró todas las representaciones de un número M por una forma F, siempre que x, y sean primos relativos. Gauss probó, además, que las formas (con un discriminante igual D) se pueden agrupar en clases.

Uno de los resultados importantes concierne a las formas compuestas: Sea $F = AX^2 + 2BXY + CY^2$ una forma que se puede transformar en el producto de dos otras formas $f = ax^2 + 2bxy + cy^2$ y $f' = a'x'^2 + 2b'x'y' + c'y'^2$ por la sustitución

$$X = p_1xx' + p_2xy' + p_3x'y + p_4yy' ,$$
$$Y = q_1xx' + q_2xy' + q_3x'y + q_4yy' ,$$

entonces F se dice *transformable* en ff'. Si además los números

$$p_1q_2 - q_1p_2,\ p_1q_3 - q_1p_3,\ p_1q_4 - q_1p_4,\ p_2q_3 - q_2p_3,\ p_2q_4 - q_2p_4 \text{ y } p_3q_4 - q_3p_4$$

no poseen un divisor común, F se llama una *compuesta* de las formas f y f'.

Gauss probó que si f y g pertenecen a la misma clase y f' y g' pertenecen a la misma clase, entonces la forma compuesta de f y f' pertenece a la misma clase como la forma compuesta de g y g'.[65]

El trabajo de Gauss con las formas pretendía dotarle de medios para encontrar resultados sobre los números enteros; los mecanismos algebraicos y abstractos le interesaban en función de los resultados concretos en la aritmética.[66]

Por último, en 1830, en la reseña de un libro llamado *Göttingische Gelehrte Anzeigen*, escrito por Ludwig Seeber, Gauss dio una representación geométrica de

[64] Un interesante estudio histórico sobre la génesis de la teoría de las formas cuadráticas, así como una breve reseña sobre los desarrollos posteriores iniciados por Gauss en las *Disquisitiones Arithmeticae*, es el de Víctor Albis: "Fermat and his problems III", *Bol Mat.* **10** (1976), no. 1–6, pp. 86–95; esta es la tercera parte de tres artículos sobre la historia de la teoría de números.

[65] Véase esta reseña en Kline, *Op. cit.* pp. 826–829.

[66] Por ejemplo, es lo que se manifiesta cuando Gauss prueba que todo número de la forma $4n + 1$ puede ser representado como la suma de cuadrados en una única manera. Consúltese Kline, *Op. cit.* p. 828.

sus formas y de las clases de formas, comenzando así la llamada teoría geométrica de números, que luego sería desarrollada por Minkowski.[67]

Vamos ahora a completar nuestra introducción mencionando algunos aspectos de la obra no aritmética de Gauss así como otros de naturaleza personal, que nos permiten una mejor comprensión del trabajo de Gauss.

Resulta aquí interesante comparar la personalidad de Gauss con otro gran matemático del siglo XIX: Cauchy. A diferencia de Gauss, Cauchy publicaba rápidamente una vez que hubiera obtenido un resultado. Boyer sugiere que esta fue tal vez la razón por la que en la historia se atribuye más la introducción del rigor a Cauchy que a Gauss, a pesar de la extraordinaria precisión lógica de los trabajos de éste.

Por otra parte, Cauchy tenía una vocación pedagógica y le gustaba enseñar; publicaba continuamente en el *Journal* de la Ecole Polytechnique así como en las *Comptes Rendus* de la Académie. Gauss no tenía mucho interés en la docencia.

Los trabajos de Cauchy resultaron muy fructíferos para las matemáticas del siglo XIX y, de forma igual que Gauss, Cauchy poseía una percepción moderna de ellas. A manera de ejemplo: la integración del siglo XVIII era tratada como la inversa de la derivación, mientras que en la aproximación de Cauchy se planteaba como el límite de una suma: esta aproximación produciría mayor riqueza en la evolución posterior de la integración.[68]

Cauchy contribuyó a casi todos los temas de la matemática como Gauss, aunque no tanto en la teoría de números. Sin embargo, fue Cauchy quien dio la primera prueba general al teorema de Fermat que establece que todo entero positivo es la suma de a lo sumo tres números triangulares o cuatro cuadrados o cinco números pentagonales o seis exagonales, y así indefinidamente. Como señala Boyer, de esta forma se daba un clímax al estudio de los números figurados que había comenzado con los pitagóricos hace más de 2000 años.[69] Entre Gauss y Cauchy no existió una relación muy cordial.

Aunque Gauss no prestó mucho interés a la geometría, lo que hizo fue genial: por una parte, en 1827, publicó un tratado con el que se inició la geometría diferencial: *Disquisitiones generales circa superficies curvas*[70], y, en 1824, estableció

[67] Cfr. Kline, *Op. cit.* p. 829.

[68] Véase Boyer, *Op. cit.* p. 564.

[69] *Ibid.*, p. 567.

[70] Su aproximación es aquí diferente de la de Monge, pues conecta consideraciones prácticas con análisis teórico más sutil; véase Struik, *A concise...*, p. 142.

sus conclusiones sobre el postulado de las paralelas. Si hubiera desarrollado y publicado estas ideas habría obtenido el crédito como el padre de la geometría no euclidiana.[71]

La obra matemática y científica de Gauss resulta impresionante.[72] Después de escribir las *Disquisitiones Arithmeticae* se dedicó al cálculo astronómico. Gauss creó el método y el procedimiento para calcular órbitas celestes con base en ciertos datos observacionales. Esto se codificó en su libro *Theoria motus corporum coelestium in sectionibus conicis solem ambientium* de 1809. Aquí trató las llamadas "perturbaciones" y brindó las técnicas que dirigirían la astronomía computacional hasta un tiempo muy reciente. Posteriores observaciones sobre los planetas Ceres, Pallas, Vesta, Juno, etc., confirmaron la precisión de los métodos de Gauss.[73] No obstante, dice Bell que—en esencia—ningún descubrimiento matemático se encuentra en *Theoria motus*.[74]

En 1811 Gauss escribía a Bessel un resultado extraordinario en el campo de los números complejos: para que la integral de línea de una función compleja sea cero es suficiente que la función sea analítica en todo punto de la curva y dentro de la curva. Este resultado no fue publicado por Gauss, como tantos otros resultados. Años después, Cauchy lo redescubriría y junto con otros resultados empujaría hacia adelante el análisis complejo del siglo XIX.[75]

En 1812 Gauss publicó un trabajo sobre las series hipergeométricas, estableciendo las restricciones para definir la convergencia de las mismas. De una manera general, de nuevo, daba tratamiento a las principales series que aparecían en la física matemática de su tiempo; con su trabajo se pudieron tratar muchas de las ecuaciones diferenciales de la física del siglo pasado.[76]

Sólo a partir de 1820 Gauss se dedicó a la investigación en Geodesia, la base aplicada de lo que sería la geometría diferencial.

---

[71] Struik afirma que Gauss estaba en posesión de la geometría no-euclidiana desde 1816; véase *A concise...*, p. 143.

[72] Un resumen formidable de la producción matemática de Gauss se puede ver en la conferencia del famoso matemático francés del grupo Bourbaki, Jean Dieudonné, que se publicó como "L'oeuvre mathématique de C. F. Gauss", París: Université de París, 1962.

[73] Cfr. Kramer, *Op. cit.* p. 475.

[74] Véase Bell, *Op. cit.* p. 242.

[75] *Ibid.*, pp. 250–251.

[76] *Ibid.*, p. 252.

Después Gauss hizo descubrimientos en la teoría electromagnética y en la teoría de la atracción newtoniana, creando la llamada teoría del potencial.[77]

Edna Kramer afirma que la contribución de Einstein a la física moderna fue posible sólo gracias a algunos de los grandes avances matemáticos que hizo Gauss.[78] En efecto, la geometría diferencial desarrollada sustancialmente después de Gauss por Riemann fue esencial para la formulación de la teoría de la relatividad. Pero además: se puede afirmar una conexión teórica interesante entre Gauss y Einstein: la idea de la relatividad nace en Einstein después de dos años de trabajar con el cálculo tensorial realizado por dos matemáticos italianos, Ricci y Levi-Civita, ambos discípulos de Riemann y Christoffel, quienes fueron inspirados por el trabajo geométrico de Gauss.[79]

Es interesante señalar también que Gauss había anticipado el teorema que el número de primos menores que un entero determinado n, tiende a $n/\ln n$, cuando n tiende a infinito, resultado al que Legendre se acercó mucho; sin embargo, no sabemos si Gauss poseía una prueba cuando escribió el resultado en una tabla de logaritmos que había obtenido a la edad de 14 años.[80, 81]

La obra de Gauss y la evolución de su trabajo se pueden recapitular a partir de un pequeño diario intelectual que se mantuvo escondido en los papeles de la familia hasta 1898; consta de 19 páginas y en él aparecen 146 enunciados de resultados, el último del 9 de julio de 1814.[82] Es este diario la principal fuente documental para demostrar la preeminencia de Gauss en el descubrimiento de tantos resultados

---

[77] Este es el significado de su obra *Allgemeine Lehrsätze*, acerca de la teoría de fuerzas que actúan inversamente proporcionales al cuadrado de la distancia; desarrollada en 1839 y 1840. Cfr. Struik, *A concise...*, p. 143.

[78] Véase Kramer, *Op. cit.* p. 473.

[79] Consúltese Bell, *Op. cit.* p. 256.

[80] El teorema de los números primos fue demostrado en 1896 por el matemático francés Jacques Hadamard (1865–1963) y el belga Charles J. de la Vallée Poussin (1866–1962). Algunas modificaciones y simplificaciones de la prueba del famoso teorema fueron dadas por German Landau (1877–1938) y otros. Luego, en 1932 Norbert Wiener dedujo una prueba más simple a partir de algunos de sus descubrimientos que G. H. Hardy llamó los "teoremas Tauberianos". Véase Kramer, *Op. cit.* pp. 503–504. Otros aspectos de la contribución de Gauss a la teoría analítica de números se estudia en un artículo poco conocido de E. Van der Blij, "Gauss and analytic number theory", en *Nieuw Tijdschr. Wisk.* **64** (1976–1977), no. 4, pp. 184–187.

[81] Sobre la historia del teorema del número primo, puede verse el artículo relativamente reciente de L. J. Goldstein "A history of the prime number theorem", *Amer. Math. Monthly* **80** (1973), pp. 599–615.

[82] Véase Boyer, *Op. cit.* p. 547.

matemáticos que no fueron publicados.[83]

Cuando se estudia la historia de las matemáticas del siglo XIX sucede un asunto curioso: siempre que se analiza un descubrimiento debe cotejarse con el diario o los papeles no publicados de Gauss para establecer si Gauss no lo había encontrado primeramente.[84, 85] Kronecker decía en el siglo pasado: "casi todo lo que las matemáticas de nuestro siglo ha producido en cuanto a ideas científicas originales, está conectado con el nombre de Gauss".[86]

¿Por qué no publicaba Gauss como otros científicos y se guardaba para sí tantos y formidables resultados matemáticos? Si se elimina la interpretación del rechazo de la academia francesa con las *Disquisitiones Arithmeticae* que se ha dicho dotó a Gauss de un celo extralimitado para publicar, pareciera que la clave se encuentra en el lema fundamental de Gauss: *"Pauca sed matura"* (pocos pero maduros). La obsesión por la perfección así como un excesivo ensimismamiento pueden dar cuenta de este asunto: de hecho, Gauss nunca tuvo mucho interés en la trasmisión del conocimiento y la enseñanza; su investigación era una experiencia individual que le proporcionaba satisfacción a sí mismo y nada más. Si Gauss hubiera tenido otro tipo de actitud es probable que las matemáticas del siglo XIX hubieran avanzado de una forma diferente, permitiendo que otros excelentes cerebros de la época no tuvieran que dedicar tantos esfuerzos y tiempo a resultados que ya Gauss había obtenido, ampliando considerablemente los alcances de la producción matemática.

La coherencia y la unidad intelectual presentes en las *Disquisitiones Arithmeticae* nos brindan un tema para hacer una reflexión sobre el método en la construcción matemática. Gauss reconstruye y sistematiza los resultados disponibles, elabora una colección de mecanismos y teorías generales, y luego da cuenta de los problemas particulares, llegando a incluir en su trabajo su resultado famoso del 17-gono regular. Se

---

[83] En 1901 este diario fue publicado por Felix Klein en un libro que celebraba el sesquicentenario de la Sociedad Científica de Göttingen.

[84] *Ibid.* p. 554.

[85] Por ejemplo, uno de los resultados más importantes que encontró Gauss y que no fue publicado es el de las funciones elípticas: al parecer Gauss conocía en 1797 la doble periodicidad de la función lemniscata, y a principios del siglo pasado ya conocía las funciones doblemente periódicas generales, con lo que se adelantaba a Abel en casi 25 años; véase Bell, E. T. *Historia de las matemáticas*, México: Fondo de Cultura Económica, 1985; p. 411. (La primera edición es de 1940 con el título *The Development of Mathematics*, New York, McGraw Hill Book Co.).

[86] Citado en el libro de D. E. Smith: *History of Mathematics*, New York: Dover Publications, 1951; p. 504. (La primera edición es de 1923).

trata de una exposición intelectualmente seria y profunda, aunque tal vez deba mencionarse que la emersión de los problemas a los que se enfrentó y resolvió con tanta destreza y generalidad los había estudiado de manera particular; es decir, en nuestra opinión, Gauss abordó los problemas individuales y construyó a partir de ellos el marco teórico que los englobaba y reducía a lo particular precisamente; la exposición en las *Disquisitiones Arithmeticae* sigue una línea de lo abstracto y general a lo particular, pero esta lógica no debería confundirse con la "lógica" heurística e intuitiva de la construcción intelectual que le permitió llegar a esos resultados generales y que siempre está presente en la construcción matemática y científica en general.

Durante los siglos XVII y XVIII la teoría de números sumaba una colección de resultados particulares y disconexos, sin un marco que les brindara coherencia. Gauss transformó esa situación convirtiendo la teoría de números en una ciencia matemática plena.[87]

Aunque siempre conviene enfatizar la importancia de la relación entre matemáticas y la realidad física, en sus múltiples dimensiones, también tiene trascendencia entender el papel de los aspectos más abstractos y "puros" de esta ciencia. La matemática cuenta como una de sus características más especiales con esa doble naturaleza de abstracción y empirismo-intuicionismo; es decir, existe un flujo creador y edificante entre las matemáticas más intuitivas físicamente (para no decir el término muy manido de "aplicadas") y las puras. En la historia de las matemáticas a veces han dominado unas dimensiones, a veces otras; en ocasiones el dominio de una de esas dimensiones ha sido determinante para hacer progresar las matemáticas en su conjunto, para ampliar sus horizontes, para solidificar su fisonomía cognitiva e intelectual, para abrir nuevas vías en la creación mental, para descubrir nuevos secretos. La relación con la física jugó un papel singular con Newton y las matemáticas del siglo XVIII. Pero también la creación de la Teoría de Números por Gauss, con su tratamiento abstracto y puro[88], contribuyó a abrir camino a la matemática moderna que dominaría el siglo XIX y penetraría en el siglo XX.

Durante casi 20 años Gauss dedicó la mayoría de su tiempo a cálculos astronómicos.[89] Tal vez se pueda lamentar que su cerebro extraordinariamente dotado no se hubiese dedicado al pensamiento abstracto más tiempo y menos a este tipo de cómputos que aunque con mayor dificultad otras personas podrían haber realizado.[90]

---

[87] Véase Bell, *Op. cit.* p. 236.

[88] Aunque en la teoría de números el tratamiento fue aritmético, y no algebraico.

[89] Cfr. Bell, *Op. cit.* p. 241.

[90] *Idem.*

Es cierto, pero también debe decirse que su involucramiento en la astronomía y el cálculo como una de sus dimensiones le permitió a Gauss una posición de reconocimiento científico e intelectual internacional que le daba medios para vivir e investigar, así como, por otra parte, su interrelación con dimensiones más empíricas de la ciencia le daba elementos teóricos para estimular su creación matemática y científica de una manera integral. A veces la visión del matemático "purista" de nuestra época juzga con su actitud reduccionista la construcción matemática del pasado, distorsionando su realidad.

Gauss estaba dotado de una genialidad matemática combinada con una extraordinaria habilidad para la experimentación empírica. Incluso, creó varios aparatos útiles en el curso de sus investigaciones: el heliotripo, para trasmitir señales luminosas, el magnetómetro, y el famoso telégrafo eléctrico (en 1833).[91]

Para dar una visión más completa de Gauss desde un punto de vista humano, vale la pena mencionar los pasatiempos que tenía: la literatura europea y clásica antigua, interés en el conocimiento de la política internacional, el dominio de lenguas extranjeras, así como la incursión en las nuevas ciencias.[92] Gauss era, si se quiere, una persona conservadora que nunca salió de su país, aunque seguía con cierto detenimiento el acontecer europeo a través de los periódicos y libros; le molestaba cualquier cosa que pudiera obstaculizar o interrumpir su trabajo, que constituía su principal fuente de satisfacción. En la década de sus treinta años Gauss no tuvo muchas fuentes de satisfacción vital y, más que eso, el infortunio lo rodeó: murió su benefactor, el Duque de Brunswick, Alemania se encontraba hundida bajo la bota napoleónica y, además, murió su primera esposa.[93] Pero con el tiempo fue reconstruyendo su vida, estableciendo sus rutinas y sus propósitos intelectuales de una manera armónica; su madre lo acompañó hasta la muerte de ésta, atendida hasta el final por Gauss, quien tal vez agradecía con su actitud la lucha que su madre dio para sacarle del medio social y cultural del que su padre no quería que saliera.

Las matemáticas del siglo XIX sufrieron una gran transformación como producto de varios resultados teóricos: entre ellos las geometrías no-euclidianas y los cuaterniones. En realidad, la esencia de este revolucionario proceso fue la ruptura con la matemática "sensible" e intuitiva, euclidiana y física que tenía lugar hasta entonces, y que Kant—por ejemplo—condensó en su filosofía asumiéndola como

[91] *Ibid.*, p. 255.

[92] *Ibid.*, p. 256.

[93] *Ibid.*, pp. 240–241.

premisa ontológica. Esto se rompió con una nueva matemática que fundamentaba su validez en el discurso lógico, combinando rigor y abstracción, aunque sufriera un "distanciamiento" de lo real intuitivo. Aquí nace la matemática moderna: con sus virtudes y sus vicios.[94]

Se debe enfatizar el carácter *revolucionario*[95] de la perspectiva de Gauss en su trabajo matemático; no se trataba de la ampliación de resultados de una manera lineal y acumulativa, era más que eso. El trabajo de Gauss representaba una nueva actitud que reformaba la práctica matemática en dimensiones muy importantes, que recolocaba los resultados obtenidos en una nueva dirección, transformando cualitativamente lo que existía antes y permitiendo nuevos derroteros.[96]

Esto hizo de Gauss el dueño de la perspectiva intelectual e histórica más avanzada en los matemáticos de su tiempo. Gauss llegó a resultados que definían un nuevo camino y una nueva estructuración de las matemáticas; sin duda, esta perspectiva y su gran talento matemático creaban las condiciones para hacer la nueva matemática con mayor propiedad que muchos otros: Gauss sabía hacia dónde apuntar y dirigir sus esfuerzos. No es extraño que encontrara tantos resultados en tantos campos antecediendo durante muchos años al resto de los matemáticos.

Aunque su preocupación por el rigor desde un principio fue decisiva para cristalizar su visión intelectual de las matemáticas, también participó su madurez para captar lo extraño y lo nuevo.

La "ruptura" con las matemáticas post-newtonianas del siglo XVIII no fue asumida por otros grandes matemáticos como Laplace o Legendre en el mismo

---

[94] Incluso, se puede considerar a Gauss el primer matemático del siglo XIX que establece una clara distinción entre aritmética y geometría; haciendo de la primera verdades lógicas y de la segunda verdades fundamentadas en la experiencia; y contribuye con ello a una separación entre las matemáticas puras y las aplicadas. Véase esta opinión en el libro de León Brunschvicg: *Les Etapes de la philosophie mathématique*, Paris: Blanchard, 1981; p. 497. (La primera versión es de 1912, en la *Revue du Mois*). La distinción que hace Gauss (que puede verse en una carta a Bessel del 9 de abril de 1830) no disminuye la extraordinaria unidad de dimensiones empíricas y teóricas presente en la práctica matemática de Gauss y que, más bien, no ha sido leída apropiadamente por muchos de los matemáticos y filósofos de nuestros días.

[95] Para una interesante discusión sobre la existencia de revoluciones en las matemáticas puede consultarse el libro de I. Bernard Cohen: *Revolution in Science*, Cambridge, E.U.A.: Harvard University Press, 1985; pp. 505–507.

[96] Sobre los componentes de la práctica científica necesarios para la interpretación histórica, puede consultarse el artículo de Angel Ruiz Zúñiga: "Problemas de método en la historia de la ciencia" en el libro editado por el mismo autor: *Las Matemáticas en Costa Rica, Memorias del Tercer Congreso Nacional de Matemáticas*, San José: 1990.

siglo XIX; muchos siguieron siendo matemáticos "del siglo XVIII"[97]. Gauss fue el primer matemático de las nuevas matemáticas que nacen el siglo pasado. Sin embargo, a pesar del sentido de apuntalamiento de lo general y abstracto que Gauss imprimió a sus trabajos, nunca dejó de tener una visión de las matemáticas asida a la realidad y al mundo; para Gauss las matemáticas nacían de problemas específicos que podían ser tratados de manera general; encontraba motivación en ellos. Su trabajo en varias partes de la física-matemática no puede verse simplemente como una necesidad pecuniaria, sino más bien en la visión y la actitud que este tenía frente a las matemáticas. En este sentido, Gauss podría considerarse menos moderno que Galois, Hamilton o Grassmann.[98] Podríamos decir que Gauss se quedaba en un término medio entre la matemática empírica del siglo XVIII y la matemática "libre y pura" de los últimos 150 años. En nuestro tiempo, después de tantos años recorridos de la matemática moderna, tal vez podamos reevaluar intelectualmente aquel término "medio" de Gauss, extraer un nuevo sentido en la naturaleza de las matemáticas[99] y vislumbrar mejor las matemáticas del futuro.

[97] Tal vez pueda señalarse a Lagrange como un precursor de la nueva visión de las matemáticas en su consideración abstracta y general de la mecánica, aunque no tuvo realmente éxito.

[98] Esta es la opinión de Bell en su libro *Historia de las Matemáticas*.

[99] Sobre una nueva visión de la naturaleza de las matemáticas constructivista y empiricista, que afirma una relación íntima de las matemáticas con el mundo físico y social puede consultarse el libro de Angel Ruiz Zúñiga: *Matemáticas y Filosofía, Estudios Logicistas*, San José: Editorial Universidad de Costa Rica, 1990.

CONTENIDOS POR ARTICULO.

En la siguiente tabla los traductores indicamos los contenidos de cada artículo de las Disquisitiones Arithmeticae. *Para ayudar al lector, nos permitimos utilizar lenguaje moderno, es decir, se usan términos introducidos después del tiempo de Gauss.*

SECCION PRIMERA. DE LA CONGRUENCIA DE LOS NUMEROS EN GENERAL.

Artículo 1. Definición de *congruente*, *módulo* y *residuo.*
2. Clases módulo m; notación para congruencias.
3. Las clases módulo m forman una partición de los enteros.
4. Residuos mínimos.
5. Congruencias según módulos compuestos; transitividad de congruencias.
6. Sumas de números congruentes.
7. Múltiplos de números congruentes.
8. Productos de números congruentes.
9. Polinomios de números congruentes.
10. Período de un polinomio módulo m.
11. Criterio necesario para resolver polinomios racionales.
12. Aplicaciones de la teoría a las reglas de aritmética elemental.

SECCION SEGUNDA. SOBRE LAS CONGRUENCIAS DEL PRIMER GRADO

13. Lema para §14.
14. Si $p|ab$ entonces $p|a$ o $p|b$.
15. Extensión de §14 a productos de varios factores.
16. Teorema fundamental de aritmética.
17. Fórmula para $\tau(A)$, el número de factores de un entero compuesto A.
18. Cálculo del máximo común divisor y mínimo común múltiplo.
19. Proposiciones elementales acerca de enteros relativamente primos.
20. Factorización primaria de una n-ésima potencia.
21. Factores de una n-ésima potencia.
22. División de una congruencia por un factor relativamente primo al módulo.
23. Si a y m son relativamente primos, a genera los enteros módulo m aditivamente.
24. Solubilidad de una congruencia lineal módulo m.
25. Congruencias trascendentales y algebraicas.
26. La solución de una congruencia consiste de varias clases de congruencia.
27. Algoritmo para resolver una congruencia lineal módulo un primo.
28. Método de Euler y Lagrange usando fracciones continuas.
29. Reducción del caso de un módulo compuesto.
30. Otro método para el caso de un módulo compuesto.
31. Cocientes módulo c.
32. Teorema chino del residuo.
33. Caso de §32 cuando los módulos son primos entre sí.
34. Posibilidad de que una congruencia sea superflua o inconsistente.
35. Ejemplo numérico del Teorema chino del residuo.
36. Otro algoritmo si los módulos son relativamente primos.
37. Sistemas de congruencias lineales.
38. Cálculo de la función $\varphi(A)$ de Euler.
39. Inversión de Möbius de la función de Euler.
40. El máximo común divisor como combinación lineal.
41. Divisibilidad de un coeficiente multinomial por un primo.
42. El lema de Gauss para un producto de polinomios con coeficientes racionales.
43. Una congruencia de grado m tiene a lo sumo m raíces.
44. Comentarios sobre el teorema de §43.

SECCION TERCERA. SOBRE RESIDUOS DE LAS POTENCIAS.

45. En el grupo multiplicativo $U(p)$ de enteros relativamente primos al módulo p, todo elemento es de orden finito menor que p.
46. Subgrupo generado por un elemento $a \in U(p)$.
47. Cálculo de potencias módulo p.
48. Si $|a| = t$ y $a^k \equiv 1 \pmod{p}$, entonces $t|k$.
49. Si p es primo, $a \in U(p)$ y $|a| = t$, entonces $t|p-1$.
50. El pequeño teorema de Fermat: $a^{p-1} \equiv 1 \pmod{p}$, un primo que no divide a a.
51. La p-ésima potencia de una suma es la suma de las p-ésimas potencias mod. p.
52. Si $d|p$, ¿cuál es el número $\psi(d)$ de elementos de $U(p)$ de orden d?
53. La prueba de que $\psi(d) = \varphi(d)$ o $\psi(d) = 0$.
54. En efecto $\psi(d) = \varphi(d)$.
55. Existencia de raíces primitivas módulo p; una segunda prueba de esto.
56. Historia de pruebas anteriores de la existencia de raíces primitivas.
57. El *índice* de un elemento b respecto a una raíz primitiva a módulo p.
58. Indice de un producto y de una potencia.
59. Indice de un cociente.
60. Cálculo de raíces módulo p.
61. Cálculo directo de raíces de la unidad módulo p: primera reducción.
62. Raíces cuadradas de la unidad.
63. Cálculo directo de raíces de la unidad: segunda reducción.
64. ¿Cuándo es -1 un residuo cuadrático?
65. Cálculo de n-ésimas raíces cuando $n|p-1$.
66. ¿Cuándo existen n-ésimas raíces de A módulo p?
67. Cálculo del orden t de A módulo p.
68. Cálculo de las demás raíces a partir de una.
69. Cambio de raíz primitiva como base.
70. Invariancia del m. c. d. del índice y $p-1$.
71. Elección de la base para que un entero tenga un índice determinado.
72. Escogencia conveniente de la raíz primitiva como base.
73. Algoritmo para encontrar raíces primitivas.
74. Ejemplo de encontrar una raíz primitiva módulo 73.
75. Producto de los elementos de un subgrupo cíclico de $U(p)$.
76. El Teorema de Wilson: $(p-1)! \equiv -1 \pmod{p}$.
77. Segunda prueba del Teorema de Wilson.
78. Generalización del Teorema de Wilson a bases compuestas.

79. Suma de los elementos de un subgrupo cíclico de $U(p)$.
80. Producto de todas las raíces primitivas.
81. Suma de todas las raíces primitivas.
82. Caso de módulos compuestos.
83. Orden de $a \in U(m)$ divide a $\varphi(M)$.
84. No hay más que t raíces t-ésimas de 1 módulo p^n.
85. Número exacto de raíces t-ésimas de 1 módulo p^n.
86. Prueba de §85: primera parte.
87. Prueba de §85: segunda parte.
88. Prueba de §85: tercera parte.
89. Cálculos con raíces primitivas módulo p^n.
90. Máximo orden en $U(2^n)$.
91. Cálculos con índices módulo 2^n.
92. Cálculos módulo un entero compuesto.
93. Trabajos de Euler sobre estos temas.

SECCION CUARTA. SOBRE LAS CONGRUENCIAS DE SEGUNDO GRADO.

94. Número máximo posible de residuos cuadráticos módulo m.
95. Definición de *residuo* y *no residuo*.
96. Número de residuos cuadráticos módulo p primo.
97. Segunda prueba de §96; ejemplos con $p \leq 17$.
98. AB es un residuo sii A y B son ambos residuos o ambos no residuos.
99. ¿Cuando un producto de varios factores es un residuo?; uso de tablas.
100. Número de residuos cuadráticos módulo p^n.
101. Si a no es divisible por p, es un residuo de p sii es un residuo de p^n.
102. ¿Cuando un entero divisible por p es un residuo módulo p^n?
103. Residuos cuadráticos módulo 2^n.
104. Número de raíces $\sqrt{A}$ si A es un residuo módulo p^n.
105. Número de raíces $\sqrt{A}$ si A es un residuo módulo m cualquiera.
106. Criterio de Euler para residuos cuadráticos.
107. Problema fundamental: dado a, encontrar todo p del cual a es un residuo.
108. -1 es un residuo de p primo sii $p = 4n + 1$.
109. Otra prueba de §108.
110. Referencia al trabajo de Euler; relación al Teorema de Wilson.
111. Caracterización de los enteros para los cuales -1 es un residuo.

112. Estudio de §107 cuando $a = \pm 2$ y $p \equiv 3$ o $5 \pmod 8$.
113. Estudio de §107 cuando $a = \pm 2$ y $p \equiv 7 \pmod 8$.
114. Estudio de §107 cuando $a = \pm 2$ y $p \equiv 1 \pmod 8$.
115. Otra prueba de §114.
116. Caracterización de los enteros para los cuales ± 2 es un residuo; historia.
117. Estudio de §107 cuando $a = \pm 3$ y $p \equiv 5$ u $11 \pmod{12}$.
118. Estudio de §107 cuando $a = \pm 3$ y $p \equiv 7 \pmod{12}$.
119. Estudio de §107 cuando $a = \pm 3$ y $p \equiv 1 \pmod{12}$.
120. Caracterización de los enteros para los cuales ± 3 es un residuo; historia.
121. Estudio de §107 cuando $a = \pm 5$ y $p \equiv 2$ o $3 \pmod 5$.
122. Estudio de §107 cuando $a = \pm 5$ y $p \not\equiv 1$ ni $9 \pmod{20}$.
123. Ley de Reciprocidad Cuadrática para $a = \pm 5$.
124. Discusión de §107 cuando $a = \pm 7$.
125. Todo $p \equiv 1 \pmod 4$ es un no residuo de algún primo $q < p$; prueba si $p \equiv 5 \pmod 8$.
126. Primer lema para probar el caso $p \equiv 1 \pmod 8$ de §125.
127. Segundo lema para probar el caso $p \equiv 1 \pmod 8$ de §125.
128. Tercer lema para probar el caso $p \equiv 1 \pmod 8$ de §125.
129. Prueba de §125.
130. Evidencia númerica para la Ley de Reciprocidad Cuadrática.
131. Enunciado de la Ley de Reciprocidad Cuadrática; notación.
132. Consecuencias de §131 con números compuestos.
133. Reciprocidad cuadrática generalizada a enteros compuestos.
134. Prueba de §133, suponiendo §131.
135. Ley de Reciprocidad Cuadrática (L. R. C.): hipótesis inductiva.
136. Prueba de L. R. C.: comienzo de la inducción; división en casos.
137. Prueba de L. R. C.: caso 1, $a \equiv p \equiv 1 \pmod 4$, $\pm pRa$.
138. Prueba de L. R. C.: caso 2, $a \equiv 1$, $p \equiv 3$, $\pm pRa$.
139. Prueba de L. R. C.: caso 3, $a \equiv p \equiv 1$, $\pm pNa$.
140. Prueba de L. R. C.: caso 4, $a \equiv 1$, $p \equiv 3$, $\pm pNa$.
141. Prueba de L. R. C.: caso 5, $a \equiv p \equiv 3$, pRb.
142. Prueba de L. R. C.: caso 6, $a \equiv 3$, $p \equiv 1$, pRb.
143. Prueba de L. R. C.: caso 7, $a \equiv p \equiv 3$, pNb.
144. Prueba de L. R. C.: caso 8, $a \equiv 3$, $p \equiv 1$, pNb.
145. Otra prueba de §114.
146. Resumen del método para determinar si Q es un residuo de P; ejemplo.

147. Formas de los divisores de $x^2 - A$: enunciado.
148. Prueba de §147 cuando $A \equiv 1 \pmod 4$.
149. Prueba de §147 cuando $A \equiv 2$ o $3 \pmod 4$.
150. Corolario de §147 con B compuesto.
151. Historia de la Ley de Reciprocidad Cuadrática.
152. Resolución de congruencias $ax^2 + bx + c \equiv 0$.

SECCION QUINTA. SOBRE LAS FORMAS Y LAS ECUACIONES INDETERMINADAS DE SEGUNDO GRADO.

153. Definición de *formas cuadráticas*; notación.
154. Representación de un número M; el determinante.
155. La raíz cuadrada $\sqrt{D}$ del determinante es una clase módulo M.
156. Representaciones que corresponden a valores iguales u opuestos de $\sqrt{D}$.
157. Transformaciones lineales de formas; formas equivalentes; transformaciones propias e impropias.
158. Equivalencia propia e impropia; ejemplo; problemas a ver.
159. Transitividad de implicación de formas; formas opuestas.
160. Formas contiguas.
161. Divisores comunes de los coeficientes de formas.
162. Encontrar todas las transformaciones de una forma a otra que la contiene.
163. Formas ambiguas.
164. Condición necesaria y suficiente para que una forma implique a otra propia e impropiamente.
165. Ejemplo de §164; existencia de una forma ambigua en una clase.
166. Representación de números por formas transformadas.
167. Determinantes de formas equivalentes.
168. Toda representación de un entero M conduce a una forma propiamente equivalente con primer coeficiente M.
169. Aplicación de la teoría de transformaciones a la de representaciones.
170. Caso de §168 con una forma ambigua.
171. Formas con determinante negativo: reducción a forma reducida.
172. Condiciones para que dos formas reducidas de determinante $-D$ sean propiamente equivalentes.
173. Condiciones para que dos formas reducidas de determinante $-D$ sean equivalentes.
174. El número de formas reducidas de determinante $-D$.
175. Clases de formas de determinante $-D$.

176. Tabla de clases de formas de determinante $-D$, $D \leq 12$.
177. Transformaciones propias entre formas contiguas.
178. Cálculo de una transformación propia entre formas propiamente equivalentes.
179. Cálculo de todas las transformaciones entre formas equivalentes.
180. Algoritmo para encontrar todas las representaciones de M por una forma de determinante $-D$.
181. Caso de §180 con coeficientes no relativamente primos.
182. Aplicación a la representación de M como $x^2 + ny^2$, $n = 1, 2, 3$.
183. Formas con determinante positivo no cuadrado: reducción a forma reducida.
184. Propiedades de formas reducidas con determinante positivo no cuadrado.
185. Algoritmos para encontrar todas las formas reducidas de determinante D.
186. Período de una forma F.
187. Propiedades de períodos; formas asociadas.
188. Sustitución $\alpha, \beta, \gamma, \delta$; ejemplo de período de una forma reducida.
189. Signos y otras propiedades de las formas en un período.
190. Lema para §191.
191. Aproximación racional a $\sqrt{D}$.
192. Convergentes de la fracción continuada de $\sqrt{D}$.
193. Formas reducidas propiamente equivalentes están en el mismo período.
194. Otra prueba del Teorema de §165.
195. Algoritmo que determina si formas del mismo determinante son equivalentes.
196. Algoritmo para encontrar una transformación propia entre formas propiamente equivalentes.
197. Relevancia de la ecuación de Pell al estudio de formas.
198. Solución fundamental de la ecuación de Pell.
199. Aplicación de fracciones continuadas a §198.
200. Solución general de la ecuación de Pell.
201. Comentarios sobre la solución de la ecuación de Pell.
202. Historia de la ecuación de Pell.
203. Algoritmo para encontrar todas las transformaciones entre formas equivalentes.
204. Observaciones sobre §203.
205. Algoritmo para encontrar todas las representaciones de un entero por una forma dada.
206. Formas reducidas con determinante h^2.
207. Toda clase contiene una sola forma reducida.
208. Encontrar una transformación entre formas equivalentes con determinante h^2.

209. Encontrar las demás transformaciones de §208.
210. Criterio para equivalencia impropia de formas reducidas $(a, h, 0)$.
211. Número de clases de formas de determinante h^2.
212. Algoritmo de §205 para el caso de formas de determinante h^2.
213. Criterio para que una forma de determinante D implique una de determinante De^2.
214. Encontrar todas las transformaciones correspondientes a §213.
215. Formas de determinante igual a cero.
216. Resolución de la ecuación cuadrática general de dos incógnitas.
217. Continuación de §216.
218. Caso de §216 con determinante cuadrado y $M = 0$.
219. Caso general de §216 con determinante cero.
220. Caso especial de §216 con determinante cero.
221. Ejemplo del método de §217.
222. Notas históricas acerca de formas cuadráticas.
223. División de las formas de determinante D en clases.
224. Usos de las clases; clases opuestas; clases ambiguas.
225. Clases positivas y negativas.
226. Formas primitivas; división de clases en órdenes; ejemplos.
227. Uso de clases propiamente primitivas.
228. Una forma primitiva representa un número infinito de enteros no divisibles por p.
229. Una forma primitiva representa sólo residuos o sólo no residuos módulo p.
230. Caracteres de una forma primitiva.
231. División de órdenes en géneros; forma principal.
232. Ejemplos con clases positivas y negativas.
233. Raíz cuadrada de una forma; números característicos de una forma.
234. Lema para §239 y §240.
235. Forma compuesta; seis propiedades.
236. Construcción de una forma compuesta.
237. Forma compuesta de formas transformadas.
238. Forma compuesta de formas equivalentes.
239. Equivalencia de las compuestas de formas equivalentes.
240. Asociatividad de composición.
241. Asociatividad generalizada de composición.
242. Propiedades de la composición de formas.

243. Clases de formas tienen la estructura de un grupo.
244. Representación de un producto por una forma compuesta.
245. Composición de órdenes.
246. Composición de géneros.
247. Producto de géneros está bien definido para formas primitivas.
248. Producto de géneros está bien definido en general.
249. Composición de clases.
250. Forma más simple de un orden.
251. Una forma primitiva que transforma formas del mismo orden.
252. Existe el mismo número de clases en cada género del mismo orden.
253. Discusión del número de clases en órdenes distintos.
254. Composición de la forma más simple de un orden con una primitiva.
255. Clases propiamente primitivas que representan un entero cuadrado.
256. Comparación del número de clases primitivas de órdenes distintos.
257. Número de formas ambiguas primitivas $(A, 0, C)$ y $(A, A/2, C)$.
258. Conteo del número de clases ambiguas propiamente primitivas.
259. Conteo del número de clases ambiguas impropiamente primitivas.
260. Número de clases propiamente primitivas k con $k^2 = K$.
261. La mitad de los caracteres no pertenece a un género propiamente primitivo.
262. Otra prueba de la L. R. C. para ciertos residuos.
263. Los caracteres que corresponden a géneros.
264. Caracteres para géneros negativos y géneros impropiamente primitivos.
265. Método para descomponer un primo como suma de dos cuadrados.

Una digresión conteniendo un estudio de formas ternarias.

266. Introducción al estudio de formas ternarias.
267. Formas ternarias: notación, adjunta y determinante.
268. Transformación de formas ternarias.
269. Formas ternarias equivalentes.
270. Transitividad de equivalencia.
271. Clases de formas ternarias; formas positivas, negativas e indefinidas.
272. Reducción de formas ternarias.
273. Ejemplos numéricos de la reducción de formas ternarias.
274. Segunda reducción de formas ternarias.
275. Ejemplos de la composición de transformaciones de formas ternarias.
276. El número de clases de formas ternarias de determinante D es finito.
277. Ejemplos de formas ternarias reducidas de determinante pequeño.

278. Problemas para considerarse acerca de formas ternarias.
279. Lema para §280.
280. Algoritmo para encontrar las representaciones propias de un entero por una forma ternaria.
281. Representaciones impropias por una forma ternaria.
282. Observaciones acerca de la representación de una forma binaria por una forma ternaria.
283. Algoritmo para encontrar todas las representaciones de una forma binaria por una forma ternaria.
284. Representaciones impropias de una forma binaria por una forma ternaria.
285. Equivalencia de formas ternarias.

Algunas aplicaciones a la teoría de las formas binarias.

286. Toda forma del género principal es el cuadrado de alguna forma.
287. Exactamente la mitad de los caracteres corresponden a géneros propiamente primitivos.
288. Existencia de formas primitivas negativas de determinante $-M$ y número característico -1.
289. Representaciones de formas binarias por $x^2 + y^2 + z^2$.
290. Estudio de §289 para formas binarias de determinante -1 o -2.
291. Las representaciones de un entero positivo por $x^2 + y^2 + z^2$.
292. Número de representaciones por $x^2 + y^2 + z^2$.
293. Todo entero positivo es la suma de tres números triangulares.
294. Condición necesaria y suficiente para resolver $ax^2 + by^2 + cz^2 = 0$.
295. Método alternativo para §294.
296. Trabajo de Legendre acerca de §294.
297. Incompletitud del argumento de Legendre en §296.
298. Caso general de §294.
299. Representación de cero por formas ternarias.
300. Solución racional de una ecuación cuadrática con dos incógnitas.
301. Comportamiento asintótico del número de géneros.
302. Comportamiento asintótico del número de clases: determinante negativo.
303. Tablas acerca de §302; conjetura sobre el número de clase.
304. Número de clases: determinante negativo.
305. Toda clase es de orden que divide al número de clases.
306. Las clases forman un grupo.
307. Algoritmo para calcular géneros y clases; ejemplos.

SECCION SEXTA. APLICACIONES VARIAS DE LAS INVESTIGACIONES PRECEDENTES.

308. Introducción y resumen de la sección.
309. Descomposición de una fracción con denominador ab.
310. Descomposición de una fracción con denominador $abc\cdots$.
311. Unicidad de la descomposición de §310.
312. Mantisa decimal de una fracción.
313. Cálculo del numerador a partir de la mantisa y del denominador.
314. Período de una fracción a/p^μ.
315. Cálculo del período de b/p^μ a partir del período de a/p^μ.
316. Comentarios sobre las tablas de los períodos de fracciones.
317. Método de cálculo de expansiones decimales en general.
318. Mantisa de una fracción en el caso general.
319. Métodos para resolver una congruencia $x^2 \equiv A \pmod{m}$.
320. Método de exclusión para la congruencia $x^2 \equiv A \pmod{m}$.
321. Números excluyentes que conviene escoger en el método de exclusión.
322. Atajos que se pueden usar en el método de exclusión.
323. Otro método para resolver $mx^2 + ny^2 = A$.
324. Uso de números excluyentes en §323.
325. Un ejemplo del método de §323 y §324.
326. Observaciones para acortar el cálculo en §323.
327. Otro método para resolver $x^2 \equiv A \pmod{M}$ cuando $A < 0$.
328. Ejemplos numéricos del método de §327.
329. Métodos de factorización de enteros: observaciones elementales.
330. Primer método de factorización: residuos cuadráticos de M.
331. Técnicas para la aplicación de §330.
332. Tres métodos para encontrar los residuos cuadráticos de M.
333. Segundo método de factorización: valor de $\sqrt{-D} \pmod{M}$.
334. Aplicaciones de §333.

SECCION SETIMA. ECUACIONES QUE DEFINEN SECCIONES DE UN CIRCULO.

335. Introducción a la ciclotomía; generalizaciones futuras posibles.
336. Reducción al caso de la división del círculo en p (primo) partes.
337. Las raíces de $x^n - 1$ son $\exp(2\pi k/n) = \cos(2\pi k/n) + i\,\mathrm{sen}(2\pi k/n)$.
338. La fórmula de Newton para la suma de las λ-ésimas potencias de las raíces.

339. La estructura cíclica de las raíces Ω de un polinomio ciclotómico X.
340. Sustitución de raíces de un polinomio ciclotómico en un polinomio.
341. Irreducibilidad de polinomios ciclotómicos sobre los racionales.
342. Factorización del polinomio ciclotómico depende de $p-1$.
343. Subgrupos y clases laterales de las raíces de un polinomio ciclotómico.
344. Clases laterales de Ω forman una partición.
345. Productos de períodos en Ω.
346. Grado de subextensiones del campo ciclotómico.
347. Sustitución de un período en un polinomio simétrico.
348. Coeficientes de un polinomio son funciones simétricas de las raíces.
349. Aplicación del Teorema de Newton al cálculo de los coeficientes.
350. Generalización de §347 con subperíodos.
351. Cálculo de polinomio mínimo de un período; ejemplo $n = 19$.
352. Algoritmo para encontrar las raíces de un polinomio ciclotómico.
353. Cálculo completo de §352 cuando $n = 19$.
354. Cálculo completo de §352 cuando $n = 17$.
355. Uso de números complejos en §352.
356. Cálculo de sumas gaussianas.
357. El polinomio ciclotómico se descompone como $\frac{1}{4}(y^2 \mp pz^2)$.
358. Distribución de las raíces Ω en tres períodos.
359. Conjetura de la imposibilidad de resolver polinomios de grado ≥ 5 por radicales.
360. Uso de resolventes de Lagrange para resolver el polinomio ciclotómico.
361. Cálculo de $\operatorname{sen}\omega$ y $\cos\omega$ donde $\omega = 2\pi k/n$.
362. Cálculo de las otras funciones trigonométricas de ω.
363. Factorización del polinomio con raíces $\operatorname{sen} k\omega$, etc.
364. Observaciones sobre §363; automorfimos de una extensión; ejemplos.
365. Se construye un p-gono sii p es un primo de Fermat.
366. Caracterización de los n para los cuales el n-gono es construible.

AL SERENISIMO

PRINCIPE Y SEÑOR

CARLOS GUILLERMO FERNANDO

DUQUE DE BRUNSWICK Y LUNEBURG

SERENISIMO PRINCIPE

Considero como mi mayor fortuna que VOS me permitáis adornar este trabajo con VUESTRO honorabilísimo nombre. Estoy obligado por un sagrado deber a ofrecéroslo a VOS. Si no fuera por vuestro favor, Serenísimo Príncipe, no habría realizado mi primer acercamiento a las ciencias. Si no fuera por VUESTROS beneficios incesantes en apoyo de mis estudios, no habría estado en capacidad de dedicarme completamente a mi apasionado amor, el estudio de las matemáticas. Ha sido exclusivamente VUESTRA generosidad la que me ha permitido liberarme de otras preocupaciones, dedicarme muchos años a la contemplación y estudio fructíferos, y finalmente darme la oportunidad de anotar en este volumen algunos de los resultados de mis investigaciones. Cuando al fin estuve preparado para presentar mi trabajo al mundo, fue exclusivamente VUESTRA munificencia la que removió todos los obstáculos que retardaron continuamente su publicación. Tanta ha sido VUESTRA generosidad hacia mí y mis esfuerzos que más bien puedo admirarla con espíritu agradecidísimo y admiración silenciosa que celebrarla con los encomios justamente merecidos. Porque no sólo me siento difícilmente a la altura de este oficio, sino también todos conocen VUESTRA extraordinaria liberalidad hacia todo

aquél que se dedica a las disciplinas superiores. Todos saben que VOS nunca habéis excluido de VUESTRO patrocinio a aquellas ciencias que comúnmente son vistas como demasiado recónditas y demasiado alejadas de la vida ordinaria. VOS MISMO en VUESTRA suprema sabiduría estáis bien enterado del íntimo y necesario lazo que une a todas las ciencias entre sí y con cualquier cosa que atañe a la prosperidad de la sociedad humana. Por ende, presento este libro como un testimonio de mi profundo respeto hacia VOS y de mi dedicación a la más noble de las ciencias. Serenísimo Príncipe, si VOS juzgáis merecedor del extraordinario favor que siempre me habéis prodigado, me congratularé de que mi trabajo no haya sido en vano y de que haya sido favorecido con un honor que aprecio por encima de todos los demás.

SERENISIMO PRINCIPE

Brunswick, en el mes de julio de 1801

De Vuestra Alteza, el más dedicado servidor

C.F. GAUSS

PREFACIO.

Las investigaciones contenidas en este volumen pertenecen a la parte de la Matemática que trata de los números enteros, y a veces de las fracciones pero nunca de los irracionales. El análisis llamado indeterminado o Diofántico que muestra la forma de seleccionar de entre las infinitas soluciones de un problema indeterminado aquéllas que son enteras o al menos racionales (usualmente con la condición adicional que deben ser positivas) no es la disciplina a la cual nos referimos, sino más bien a una parte verdaderamente especial, relacionada con ella en términos generales como se relaciona el arte de reducir y resolver ecuaciones (Algebra) con el Análisis general. Tal como incluimos bajo el título *Análisis* todas las discusiones que involucran cantidades, así los enteros (y las fracciones en tanto que están determinadas por enteros) constituyen el objeto propio de la ARITMETICA. Sin embargo, lo que comúnmente es llamado Aritmética, escasamente se extiende más allá del arte de enumerar y calcular (i.e., expresar los números mediante símbolos idóneos, por ejemplo, por una representación decimal, y llevar a cabo operaciones aritméticas). A menudo incluye algunos temas que realmente no pertenecen a la Aritmética (como la teoría de logaritmos) y otros que no son propios de los enteros sino comunes a todas las cantidades. Se ve como resultado que se debe dividir la Aritmética en dos partes: la Aritmética Elemental y la Aritmética Superior. La segunda incluye todas las investigaciones generales acerca de las propiedades especiales de los enteros, y es la única que tratamos en este volumen.

Incluidos bajo el título Aritmética Superior están aquellos tópicos que Euclides trató en Libros VII y siguientes de los Elementos con la elegancia y el rigor habitual entre los antiguos, pero están limitados a los rudimentos de la ciencia. La célebre obra de Diofanto, dedicada totalmente a problemas indeterminados contiene muchos resultados que provocan una apreciación más allá de lo ordinario por la ingeniosidad y habilidad del autor, a causa de las dificultades que enfrentó y los sutiles artificios que usó, especialmente si consideramos las pocas herramientas que pudo usar. Sin embargo, demandan una cierta destreza y una manipulación hábil más que principios profundos, y dado que las cuestiones son muy especializadas y rara vez conducen

a conclusiones más generales, se ve que el libro de Diofanto marca una época en la historia de las Matemáticas, más debido a que presenta los primeros trazos del arte característico del Algebra que a causa de que haya enriquecido la Aritmética Superior con nuevos descubrimientos. Se debe mucho más a los autores modernos, de los cuales aquellos pocos hombres de gloria inmortal, P. DE FERMAT, L. EULER, L. LAGRANGE, A. M. LEGENDRE (y otros pocos) abrieron la entrada al santuario de esta ciencia divina y revelaron abundantes riquezas dentro de él. No haremos aquí un recuento de los descubrimientos individuales de estos geómetras puesto que se pueden encontrar en el Prefacio del Apéndice que Lagrange agregó al Algebra de Euler y en el reciente volumen de Legendre (que citaremos luego). También citaremos muchos de ellos en el lugar apropiado dentro de estas Disquisiciones.

El propósito de este volumen, cuya publicación prometí hace cinco años, es divulgar mis investigaciones en la Aritmética Superior, tanto las iniciadas por aquellos días como las posteriores. Para que nadie se sorprenda porque comienzo casi desde el principio y trato nuevamente muchos resultados que ya han sido estudiados activamente por otros, debo explicar que cuando primero me encaminé a este tipo de investigaciones, a principios de 1795, no estaba al tanto de los modernos descubrimientos en el campo y no tenía los medios para descubrirlos. En efecto, ocupado en otro trabajo, me encontré con un extraordinario resultado aritmético (si no me equivoco, fue el teorema del artículo 108); puesto que lo consideré bellísimo en sí mismo y en vista de que sospeché su conexión con resultados aún más profundos, concentré en él todos mis esfuerzos, con el fin de entender los principios de los que dependía y para obtener una prueba rigurosa. Cuando tuve éxito en esto, me atrajeron tanto estos asuntos que no pude dejarlos. Así, mientras un resultado conducía a otro, había completado la mayor parte de lo que se presenta en las cuatro primeras secciones de esta obra antes que entrara en contacto con trabajos similares de otros geómetras. Una vez que estuve en capacidad de estudiar los escritos de estos hombres de genio, reconocí que la mayor parte de mis meditaciones habían sido agotadas en materias ya bien desarrolladas. Pero esto sólo me estimuló un mayor interés, y caminando sobre sus pasos intenté extender la Aritmética más allá, logrando resultados que están incorporados en las secciones V, VI y VII. Después comencé a considerar la publicación de los frutos de mis investigaciones y me dejé persuadir de no omitir ninguno de los primeros resultados, porque en ese momento no había ningún libro que pusiera juntos los trabajos de otros geómetras, dispersos como estaban dentro de los Comentarios de las Academias eruditas. Por otra parte, muchos de los resultados eran nuevos, la mayoría fueron tratados por nuevos métodos y los últimos resultados estaban tan ligados con los viejos que no podían explicarse sin repetir desde el inicio.

En el ínterin apareció un trabajo sobresaliente de un hombre a quien la Aritmética Superior ya debe mucho, "Essai d'une théorie des nombres" (Paris, año VI) de Legendre, donde él reune y sistematiza no solamente todo lo que había sido descubierto hasta esa fecha sino también muchos nuevos resultados propios. Ya que ese libro llegó a mis manos después de que gran parte de mi trabajo estaba levantado, no pude referirme a él en secciones análogas de mi libro. Sin embargo, me sentí obligado a agregar Notas Adicionales en algunos pasajes y confío que este comprensivo e ilustre hombre no se ofenderá.

La publicación de mi trabajo se vio estorbada por muchos obstáculos a lo largo de un período de cuatro años. Durante este tiempo no sólo continué investigaciones que ya había emprendido y aplazado para una fecha posterior de modo que el libro no fuera demasiado extenso, sino también acometí nuevas investigaciones. De modo semejante, muchos asuntos que asumí sólo a la ligera, porque un tratamiento más detallado parecía menos necesario (e.g., los contenidos de los artículos 37, 82 y siguientes, y otros), han sido desarrollados en mayor grado y han conducido a resultados más generales que parecen dignos de publicación (véase la Nota Adicional en artículo 306). Finalmente, ya que el libro se hizo mucho más extenso de lo que yo esperaba, debido al tamaño de la Sección V, acorté mucho de lo que primeramente intenté hacer y, en particular, omití toda la Sección *ocho* (aún cuando en ocasiones me refiero a ella en el presente trabajo; iba a contener un tratamiento general de las congruencias algebraicas de rango arbitrario). Todas estas cosas, que llenarían fácilmente un libro del tamaño de éste, se publicarán en la primera oportunidad.

En varias cuestiones difíciles he usado pruebas sintéticas y he suprimido el análisis que conduce a los resultados. Esto fue necesario por brevedad, una consideración que hubo que tener en cuenta tanto como fuera posible.

La teoría de la división de un círculo o de polígonos regulares, tratada en la Sección VII, *en sí misma* no pertenece a la Aritmética, pero los *principios* involucrados dependen exclusivamente de la Aritmética Superior. Los geómetras pueden sorprenderse de este hecho en sí, tanto como espero que estarán complacidos con los nuevos resultados que se derivan de este tratamiento.

Estas son las cosas acerca de las cuales quería prevenir al lector. No me corresponde a mí juzgar el trabajo mismo. Mi mayor esperanza es que él complazca a aquéllos que se interesan en el desarrollo de las ciencias, ya sea suministrando soluciones que ellos buscaban o abriendo el camino para nuevas investigaciones.

DISQUISITIONES ARITHMETICAE.

Sección Primera

DE

LA CONGRUENCIA DE LOS NUMEROS EN GENERAL

Números congruentes, módulos, residuos y no residuos.

1.

Si un número a divide la diferencia de los números b y c, se dice que b y c *son congruentes según el módulo* a; si no lo son, se dice que son *incongruentes*; el número a se llama *módulo*. Ambos números b y c, en el primer caso, son llamados uno *residuo* del otro y, en el segundo caso, *no residuos*.

Tales nociones valen para todos los enteros, tanto positivos como negativos*), y no para las fracciones. Por ejemplo, -9 y $+16$ son congruentes según el módulo 5; -7 es un residuo de $+15$ según el módulo 11; pero no es un residuo según el módulo 3. Dado que cada número divide a cero, todo número puede considerarse congruente consigo mismo, según cualquier módulo.

2.

Todos los residuos de un número dado, a, según el módulo m están comprendidos en la fórmula $a + km$, donde k es un número entero indeterminado. Las proposiciones más fáciles, a las cuales haremos referencia más adelante, pueden demostrarse aquí sin dificultad alguna, y quienquiera podrá comprobar su veracidad con igual facilidad.

*) El módulo debe ser siempre tomado con el valor *absoluto*, a saber: sin ningún signo.

Señalaré la congruencia de los números mediante este símbolo '$\equiv$' y, cuando sea necesario, pondré el módulo entre paréntesis; por ejemplo, $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$*).

3.

TEOREMA. *Dados m números enteros sucesivos*

$$a,\ a+1,\ a+2,\ \ldots a+m-1,$$

y dado otro entero A, uno y sólo uno de estos enteros será congruente a A según el módulo m.

Si $\frac{a-A}{m}$ es un entero, entonces $a \equiv A$; si $\frac{a-A}{m}$ es una fracción, sea k el próximo mayor entero positivo (y si es negativo, el próximo menor, sin considerar el signo). $A + km$, que estará entre a y $a + m$, será el número buscado. Es evidente que todos los cocientes $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, y $\frac{a+2-A}{m}$, etc. están ubicados entre $k-1$ y $k+1$; por lo que solo uno de ellos puede ser entero.

Residuos mínimos.

4.

Así, pues, cada número tendrá un residuo, tanto en la sucesión $0, 1, 2, \ldots m-1$, como en $0, -1, -2, \ldots -(m-1)$ a los que llamamos *residuos mínimos.* Es evidente que, a no ser que 0 sea un residuo, siempre se presentan en pares: uno *positivo* y el otro *negativo.* Si son diferentes en magnitud, uno será $< \frac{m}{2}$; de otro modo, cada uno será $= \frac{m}{2}$ sin considerar signos. De donde es evidente que cada número tiene un residuo no mayor que la mitad del módulo, al que se llamará *residuo absolutamente mínimo.*

Por ejemplo: -13 tiene, según el módulo 5, un residuo mínimo positivo que es un residuo absolutamente mínimo; -3 es el residuo mínimo negativo; $+5$ es residuo mínimo positivo de sí mismo, según el módulo 7; -2 es el residuo mínimo negativo, y a la vez, absolutamente mínimo.

*) Adoptamos este símbolo por la gran analogía que se encuentra entre la igualdad y la congruencia. Por la misma razón, el ilustre Legendre, en su tratado, usó el mismo símbolo para la igualdad y la congruencia, lo que nosotros dudamos en imitar para que no se originara ninguna ambigüedad.

Proposiciones elementales sobre congruencias.

5.

Establecidos estos conceptos, reflexionemos sobre las propiedades de los números congruentes que son inmediatamente obvias.

Los números congruentes, según un módulo compuesto, también serán congruentes según cualquier factor de este módulo.

Si varios números son congruentes a un mismo número según un mismo módulo, serán congruentes entre sí (según el mismo módulo).

Esta identidad de módulos se debe sobreentender, también, en lo siguiente:

Los números congruentes poseen los mismos residuos mínimos; los números no congruentes poseen diferentes residuos mínimos.

6.

Si se tienen los números A, B, C, etc., y otros números a, b, c, etc., que son respectivamente congruentes a ellos según un módulo cualquiera, es decir, $A \equiv a$, $B \equiv b$, etc. entonces, $A + B + C +$ etc. $\equiv a + b + c +$ etc.

Si $A \equiv a$, $B \equiv b$, entonces $A - B \equiv a - b$.

7.

Si $A \equiv a$, entonces, también $kA \equiv ka$.

Si k es un número positivo, entonces este es un caso particular del artículo anterior (art. 6), suponiendo que $A = B = C$ etc., y $a = b = c$ etc. Si k es negativo, entonces, $-k$ será positivo, de donde $-kA \equiv -ka$, de tal modo que $kA \equiv ka$.

Si $A \equiv a$, $B \equiv b$, entonces $AB \equiv ab$, pues $AB \equiv Ab \equiv ab$.

8.

Si se tienen los números A, B, C, etc., y otros números a, b, c, etc., respectivamente congruentes a aquellos, esto es si $A \equiv a$, $B \equiv b$, etc., los productos de cada uno de ellos serán congruentes, ABC etc. $\equiv abc$ etc.

Del artículo anterior, se tiene $AB \equiv ab$, y, por la misma razón, $ABC \equiv abc$, así para cualquier número de factores.

Si todos los números A, B, C, etc. se suponen iguales, y también los correspondientes a, b, c, etc., se tiene este teorema: *Si $A \equiv a$ y k es un entero positivo, entonces $A^k \equiv a^k$.*

9.

Sea X una función algebraica de la indeterminada x, de la forma

$$Ax^a + Bx^b + Cx^c + \text{ etc.}$$

donde A, B, C, etc., son números enteros cualesquiera, y donde a, b, c, etc. son enteros no negativos. Entonces, si se dan valores congruentes a la indeterminada x, según cualquier módulo entero, los valores correspondientes de la función X serán congruentes.

Sean f y g valores congruentes de x. Luego, por el artículo anterior, $f^a \equiv g^a$ y $Af^a \equiv Ag^a$, y del mismo modo $Bf^b \equiv Bg^b$, etc. Entonces,

$$Af^a + Bf^b + Cf^c + \text{ etc.} \equiv Ag^a + Bg^b + Cg^c + \text{ etc.} \qquad \textit{Q. E. D.}$$

Fácilmente se infiere cómo puede ser extendido el teorema a las funciones de varias indeterminadas.

10.

Si se sustituye x por todos los números enteros, consecutivamente, y si se reducen los valores de la función X a los residuos mínimos, entonces éstos formarán una sucesión en la que después de un intervalo de m términos (tomando a m como el módulo) los mismos términos se repetirán de nuevo. Entonces, la serie estará formada por un período de m términos repetido infinitamente. Por ejemplo, sea $X = x^3 - 8x + 6$ y $m = 5$; entonces para $x = 0$, 1, 2, 3, etc. los valores de X producen estos residuos mínimos positivos: 1, 4, 3, 4, 3, 1, 4, etc. donde los primeros cinco números 1, 4, 3, 4, 3 se repiten indefinidamente y, si la sucesión se continúa en el sentido contrario, esto es, si se dan valores negativos a x, el mismo período aparece con los términos en el orden inverso. De donde, resulta evidente que no pueden tener lugar otros términos en cualquier sucesión, excepto aquéllos que constituyen este período.

11.

Por lo tanto, en este ejemplo, X no puede ser ni $\equiv 0$, ni $\equiv 2 \pmod 5$, ni mucho menos $= 0$ ni $= 2$. De donde, se deduce que las ecuaciones $x^3 - 8x + 6 = 0$, y $x^3 - 8x + 4 = 0$ no pueden resolverse con números enteros, y, como se sabe, tampoco con racionales. Más generalmente, es evidente que, cuando X es una función de la incógnita x, de la forma

$$x^n + Ax^{n-1} + Bx^{n-2} + \text{ etc.} + N$$

donde A, B, C, etc. son enteros y n es un entero positivo (en realidad todas las ecuaciones *algebraicas* pueden reducirse a esta forma), la ecuación $X = 0$ no tiene ninguna raíz racional, si la congruencia $X \equiv 0$ no puede satisfacerse para ningún módulo. Aunque este criterio se nos presentó espontáneamente, será tratado más ampliamente en la Sección VIII. A partir de este ejemplo se puede formar alguna idea sobre la utilidad de estas investigaciones.

Algunas aplicaciones.

12.

Muchas cosas que suelen enseñarse en aritmética dependen de los teoremas expuestos en esta sección, e.g., las reglas para averiguar la divisibilidad de un número dado por 9, 11 u otro. *Según el módulo 9* todas las potencias del número 10 son congruentes con la unidad: por eso, si un número dado tiene la forma $a + 10b + 100c +$ etc., entonces dará, según el módulo 9, el mismo residuo mínimo que $a + b + c +$ etc. Así, es evidente que, si los dígitos de un número expresado en decimales se suman uno a uno sin tener en cuenta el lugar que ocupan, esta suma y el número dado presentan los mismos residuos mínimos, de tal modo que éste último puede dividirse entre 9, si aquel es divisible entre 9 y viceversa. Lo mismo es cierto para el divisor 3. Puesto que *según el módulo* 11, $100 \equiv 1$ será, en general $10^{2k} \equiv 1$, $10^{2k+1} \equiv 10 \equiv -1$, y un número de la forma $a + 10b + 100c +$ etc. dará, según el módulo 11, el mismo residuo mínimo que $a - b + c$ etc.; de donde de inmediato se deriva la regla conocida. De este mismo principio, se deducen todas las reglas similares.

De lo anterior se puede inferir el principio de las reglas dadas para la verificación de las operaciones aritméticas. Desde luego, si de los números dados, se derivan otros ya sea por suma, resta, multiplicación o elevación a potencia, se

sustituyen los residuos mínimos en lugar de los números dados, según un módulo arbitrario (por lo general se usan 9 u 11, porque como lo presentamos en nuestro sistema decimal, según éstos, los residuos pueden hallarse con facilidad). Por esto, los resultados deben ser congruentes con los que se derivaron de otros dados; porque si no sucediera así, se concluiría que se ha cometido un error en el cálculo.

Pero, puesto que estos resultados son bastante conocidos y semejantes con los anteriores, sería innecesario detenerse en ellos.

Sección Segunda

SOBRE

LAS CONGRUENCIAS DEL PRIMER GRADO

Teoremas preparatorios sobre los números primos, factores, etc.

13.

TEOREMA. *El producto de dos números positivos, más pequeños que un número primo dado, no puede dividirse por este número primo.*

Sea p primo, y a positivo $< p$: entonces no puede encontrarse ningún número positivo b menor que p tal que $ab \equiv 0 \pmod{p}$.

Demostración. Si se niega el teorema, tendremos números b, c, d, etc., todos $< p$, tales que $ab \equiv 0$, $ac \equiv 0$, $ad \equiv 0$, etc., $\pmod{p}$. Sea b el menor de todos estos, tal que ningún número menor que b tenga esta propiedad. Es evidente que $b > 1$: pues si $b = 1$, entonces $ab = a < p$ (por hipótesis) y por lo tanto no es divisible por p. Ahora, como p es primo, no puede dividirse por b pero está comprendido entre dos múltiplos sucesivos de b, mb y $(m+1)b$. Sea $p - mb = b'$; así b' será un número positivo y $< b$. Ahora, como suponemos que $ab \equiv 0 \pmod{p}$, también tenemos $mab \equiv 0$ (por art. 7), y restando éste de $ap \equiv 0$ resulta $a(p - mb) = ab' \equiv 0$; esto es: b' tiene que ser uno de los números b, c, d, etc., aunque resulta menor que el menor de tales números, b. *Q. E. A.*

14.

Si ni a ni b pueden dividirse por un número primo p, tampoco el producto ab puede dividirse por p.

Sean α y β los menores residuos positivos de los números a y b, respectivamente, según el módulo p. Ninguno de ellos es cero (por hipótesis). Ahora, si $ab \equiv 0$ (mod. p), entonces $\alpha\beta \equiv 0$, puesto que $ab \equiv \alpha\beta$. Pero esto contradice el teorema anterior.

Euclides ya había demostrado este teorema en sus *Elementos* (libro VII, No. 32). No obstante deseábamos no omitirlo puesto que muchos autores modernos han usado razonamientos inciertos en vez de demostraciones, o bien han despreciado el teorema completamente. Además, mediante este uso muy sencillo, podemos con más facilidad comprender la naturaleza del método que se usará más adelante para resolver problemas mucho más difíciles.

15.

Si ninguno de los números a, b, c, d, etc., puede dividirse por un número primo p, tampoco puede dividirse por p el producto abcd etc.

Según el artículo anterior, ab no puede dividirse por p; por lo tanto, tampoco abc, ni tampoco $abcd$, etc.

16.

TEOREMA. *Cualquier número compuesto puede resolverse en factores primos de una manera única.*

Demostración. Que cualquier número compuesto pueda resolverse en factores primos, resulta de consideraciones elementales, pero está supuesto tácitamente, y en general sin demostración, que no puede hacerse de muchas maneras diferentes. Supongamos que algún número compuesto A, que es $= a^\alpha b^\beta c^\gamma$ etc., donde a, b, c, etc. denotan números primos diferentes, es resoluble en factores primos de otra manera.

Primero, es claro que no puede aparecer en este segundo sistema de factores ningún otro primo mas que a, b, c, etc. puesto que ningún otro primo puede dividir a A, el cual está compuesto de estos primos. De forma semejante, ninguno de los primos a, b, c, etc. puede estar ausente del segundo sistema de primos, puesto que si no, no podría dividir a A (artículo anterior). Así, estas dos resoluciones en factores pueden ser diferentes solamente si un primo aparece más veces en una resolución que en la otra. Sea p un tal primo que aparece m veces en una resolución, y n veces en la otra, y tal que $m > n$. Al disminuir en n el número de factores p en cada sistema,

quedarán $m-n$ factores p en un sistema mientras que no quedará ninguno en el otro. Esto es, tenemos dos resoluciones en factores del número $\frac{A}{p^n}$. El que una de ellas no contenga al factor p mientras que la otra lo contenga $m-n$ veces contradice lo que acabamos de demostrar.

17.

Si un número compuesto A es el producto de B, C, D, etc., entonces entre los factores primos de B, C, D, etc., no puede aparecer ninguno que no sea factor de A. Además cada uno de estos factores debe aparecer en la resolución de A tantas veces como aparece en B, C, D, etc., en total. Por lo tanto tenemos un criterio para determinar si un número B divide a un número A o no. B dividirá a A siempre que contenga sólo factores primos de A mismo, y siempre que no los contenga más veces que A. Si alguna condición no se cumple, B no divide a A.

Es fácil ver por el cálculo de las combinaciones que si, como arriba, a, b, c, etc., son números primos diferentes y si $A = a^\alpha b^\beta c^\gamma$ etc., entonces A tendrá

$$(\alpha+1)(\beta+1)(\gamma+1) \quad \text{etc.}$$

divisores diferentes, incluyendo a 1 y a A mismo.

18.

Por lo tanto si $A = a^\alpha b^\beta c^\gamma$ etc., $K = k^\kappa l^\lambda m^\mu$ etc., y si los primos a, b, c, etc., k, l, m, etc., son todos diferentes, entonces es claro que A y K no tienen un factor común aparte de 1, o sea: son primos relativos.

Dados varios números A, B, C, etc., el *máximo común divisor* se determina de la manera siguiente. Supóngase que todos los números están resueltos en sus factores primos, y de estos últimos se extraen aquéllos que sean comunes a A, B, C, etc., (si no hay ninguno, no habrá un divisor común de todos ellos). Luego, se nota el número de veces que aparece cada factor primo en A, en B, en C, etc., o sea se nota cuál exponente tiene cada uno de ellos en A, en B, en C, etc. Finalmente asignamos a cada factor el más pequeño de los exponentes que tenga en A, en B, en C, etc. Al formar el producto de estos obtendremos el común divisor buscado.

Cuando deseamos el *mínimo común múltiplo*, seguimos el siguiente procedimiento: se reunen todos los números primos que dividen a alguno de los números A,

B, C, etc., y se asigna a cada uno el mayor exponente que tiene en A, B, C, etc. Al formar el producto de éstos, tendremos el múltiplo que buscamos.

Ejemplo. Sea $A = 504 = 2^3 3^2 7$, $B = 2880 = 2^6 3^2 5$, $C = 864 = 2^5 3^3$. Para el máximo común divisor tenemos los factores primos 2 y 3 con los exponentes 3 y 2 respectivamente; esto será $2^3 3^2 = 72$, y el menor número divisible por ellos en común será $2^6 3^5 5 \cdot 7 = 60480$.

Omitimos las demostraciones debido a su facilidad. Además, sabemos por consideraciones elementales cómo resolver estos problemas cuando la resolución de los números A, B, C, etc., no viene dada.

19.

Si los números a, b, c, etc., son todos primos relativos a k, también su producto será primo relativo a k.

Como ninguno de los números a, b, c, etc., tiene un factor primo común con k, y como el producto *abc* etc., no tiene factores primos diferentes de los factores primos de uno de los números a, b, c, etc., el producto *abc* etc., tampoco tendrá ningún factor primo común con k. Por lo tanto se sigue del artículo anterior que k y *abc* etc. son primos relativos.

Si los números a, b, c, etc., son primos entre sí, y si cada uno de ellos divide a algún k, entonces su producto divide a k.

Esto se sigue fácilmente de los artículos 17 y 18. Sea p un divisor primo del producto *abc* etc. que lo contiene π veces. Es claro que alguno de los números a, b, c, etc., tiene que contener este mismo divisor π veces. Luego también k, al cual este número divide, contiene π veces a p. De manera semejante sucede con los restantes divisores del producto *abc* etc.

Así, *si dos números m y n son congruentes según varios módulos a, b, c, etc., que son primos entre sí, entonces serán congruentes según el producto de ellos.*

Como $m-n$ es divisible por cada uno de los números a, b, c, etc., será divisible por su producto también.

Finalmente, *si a es primo a b y ak es divisible por b, entonces k también es divisible por b. Porque ak es divisible por ambos a y b, es divisible por ab también; es decir* $\frac{ak}{ab} = \frac{k}{b}$ *es un entero.*

20.

Cuando $A = a^\alpha b^\beta c^\gamma$ *etc., donde* a, b, c, *etc., son números primos distintos, es alguna potencia, digamos* k^n, *todos los exponentes* α, β, γ, *etc., serán divisibles por* n.

Puesto que el número k no involucra factores primos diferentes de a, b, c, etc., supóngase que k contiene el factor a, α' veces. k^n, o A, contendrá este factor $n\alpha'$ veces. Por lo tanto $n\alpha' = \alpha$ y $\frac{\alpha}{n}$ es un número entero. De igual manera se demuestra que $\frac{\beta}{n}$, etc., son números enteros.

21.

Cuando a, b, c, *etc., son primos entre sí y el producto abc etc. es alguna potencia, por ejemplo* k^n, *entonces cada uno de los números* a, b, c, *etc., será una potencia semejante.*

Sea $a = l^\lambda m^\mu p^\pi$ etc. con l, m, p, etc., números primos diferentes. Por hipótesis, ninguno de ellos es factor de los números b, c, etc. Así, el producto abc etc. contendrá λ veces el factor l, μ veces el factor m, etc. Así que (por el artículo anterior) λ, μ, π, etc., son divisibles por n y resulta que

$$\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}} \quad \text{etc.}$$

es un entero. De manera semejante para los restantes b, c, etc.

Estos teoremas sobre los números primos tenían que presentarse primero; ahora nos dedicaremos a las proposiciones propias de nuestros fines.

22.

Si los números a *y* b *son divisibles por otro número* k, *y si son congruentes según un módulo* m *que es primo a* k, *entonces* $\frac{a}{k}$ *y* $\frac{b}{k}$ *serán congruentes según el mismo módulo.*

Es claro que $a - b$ es divisible por k y además por m (por hipótesis); así que (art. 19) $\frac{a-b}{k}$ es divisible por m, o sea, $\frac{a}{k} \equiv \frac{b}{k} \pmod{m}$.

Manteniendo iguales las otras cosas, si m y k tienen un máximo común divisor e, entonces $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$, puesto que $\frac{k}{e}$ y $\frac{m}{e}$ son primos entre sí. Pero $a - b$ es divisible por k y por m, así que $\frac{a-b}{e}$ es divisible por $\frac{k}{e}$ y por $\frac{m}{e}$, entonces es divisible por $\frac{km}{e^2}$; esto es $\frac{a-b}{k}$ es divisible por $\frac{m}{e}$, lo cual implica que $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$.

23.

Si a es primo a m, y e y f, no son congruentes según el módulo m, entonces ae y af, tampoco serán congruentes según el módulo m.

Esto es simplemente el recíproco del teorema anterior.

Después de esto, es evidente que si se multiplica a por todos los números enteros de 0 hasta $m-1$, y se reduce cada producto a su menor resto según el módulo m, entonces todos serán diferentes. Como hay m de estos restos, ninguno de los cuales es $> m$, se encuentran entre ellos todos los números de 0 hasta $m-1$.

24.

La expresión $ax+b$, donde a y b son números dados y x denota un número indeterminado o variable, *puede hacerse congruente según el módulo m a cualquier número, siempre que m sea primo a a.*

Sea c el número al cual se hará congruente, y sea e el menor resto positivo de $c-b$ según el módulo m. Por el artículo anterior necesariamente se da un valor de $x < m$ tal que el menor resto del producto ax según el módulo m será e. Si este valor es v, $av \equiv e \equiv c-b$; por lo tanto $av+b \equiv c \pmod{m}$. *Q. E. F.*

25.

Llamamos *congruencia* a cualquier expresión que contiene dos cantidades congruentes como en una ecuación. Si involucra una incógnita, se dice que se *resuelve* cuando se encuentra un valor (*raíz*) que satisface la congruencia. Así es claro lo que significan una *congruencia resoluble y congruencia no resoluble.* Obviamente se pueden usar aquí las distinciones parecidas a las usadas al hablar de las ecuaciones. Ejemplos de congruencias *trascendentales* se darán más adelante. Las congruencias *algebraicas* se distribuyen según la mayor potencia de la incógnita en congruencias de primero, de segundo, y de más altos *grados.* De manera semejante se pueden proponer varias congruencias involucrando varias incógnitas, y podemos hablar de su *eliminación.*

La resolución de las congruencias del primer grado.

26.

La congruencia del primer grado $ax+b \equiv c$, según el artículo 24, siempre es

resoluble cuando el módulo es primo relativo a a. Ahora, si v es un valor conveniente de x, o sea, es una raíz de la congruencia, resulta claro que todo número congruente a v según el módulo involucrado también es raíz (art. 9). Con igual facilidad se ve que todas las raíces tienen que ser congruentes a v. De hecho si t es otra raíz, entonces $av + b \equiv at + b$, entonces $av \equiv at$, $v \equiv t$ (art. 22). Se concluye que la congruencia $x \equiv v \pmod{m}$ representa la solución completa de la congruencia.

Como todos los valores de x que son valores de la congruencia son congruentes entre sí, y como así los números congruentes pueden considerarse equivalentes, se puede considerar tales soluciones como una sola. Por lo cual, como nuestra congruencia $ax + b \equiv c$ no admite otras soluciones, diremos que tiene una, y únicamente una solución, o bien que tiene una, y únicamente una raíz. Así, por ejemplo, la congruencia $6x + 5 \equiv 13 \pmod{11}$ no admite más raíces que las que son $\equiv 5 \pmod{11}$. Esto no es cierto en las congruencias de otros grados ni en las congruencias del primer grado en las cuales se multiplica la incógnita por un número que no es primo relativo al módulo.

27.

Quedan por añadir algunos detalles sobre el cálculo de la solución de alguna congruencia. Primero notamos que una congruencia de la forma $ax + t \equiv u$, donde suponemos que el módulo es primo a a, depende de $ax \equiv \pm 1$. Porque si $x \equiv r$ satisface esta última, $x \equiv \pm(u - t)r$ satisfará la penúltima. Pero la congruencia $ax \equiv \pm 1$, cuyo módulo se denota por b, es equivalente a la ecuación indeterminada $ax = by \pm 1$. Como hoy en día es conocida la resolución de ella, basta presentar el algoritmo para su cálculo.

Si las cantidades A, B, C, D, E, etc., dependen de α, β, γ, δ, etc., de tal manera que

$$A = \alpha, \quad B = \beta A + 1, \quad C = \gamma B + A, \quad D = \delta C + B, \quad E = \epsilon D + C, \text{ etc.}$$

por brevedad las escribimos así:

$$A = [\alpha], \quad B = [\alpha, \beta], \quad C = [\alpha, \beta, \gamma], \quad D = [\alpha, \beta, \gamma, \delta], \quad \text{etc.*)}$$

*) Esta relación puede considerarse con más generalidad, como lo haremos en otra ocasión. Aquí solamente añadiremos dos proposiciones que serán útiles para nuestras investigaciones, a saber: 1º. $[\alpha, \beta, \gamma, \ldots, \lambda, \mu] \cdot [\beta, \gamma, \ldots, \lambda] - [\alpha, \beta, \gamma, \ldots, \lambda] \cdot [\beta, \gamma, \ldots, \lambda, \mu] = \pm 1$

Ahora consideramos la ecuación indeterminada $ax = by+1$, donde a y b, son positivos. Podemos suponer sin pérdida de generalidad que a no es $< b$. Ahora, mediante el algoritmo conocido para calcular el máximo común divisor de dos números, formamos a través de la división ordinaria las ecuaciones

$$a = \alpha b + c, \quad b = \beta c + d, \quad c = \gamma d + e, \quad \text{etc.},$$

así que α, β, γ, etc., c, d, e, etc., son enteros siempre positivos, y b, c, d, e, decrecen hasta que encontramos $m = \mu n + 1$, algo que eventualmente debe ocurrir. Así resulta

$$a = [n, \mu, \ldots, \gamma, \beta, \alpha], \qquad b = [n, \mu, \ldots, \gamma, \beta].$$

Si tomamos $\qquad x = [\mu, \ldots, \gamma, \beta], \qquad y = [\mu, \ldots, \gamma, \beta, \alpha]$

tendremos $ax = by + 1$ cuando el número de términos α, β, γ, $\ldots \mu$, es par, o bien $ax = by - 1$ cuando es impar.

28.

El ilustre Euler fue el primero en dar la resolución general para las ecuaciones indeterminadas de este tipo (*Comment. Petrop. T.* VII. *p.* 46). El método que él usó consistía en sustituir x e y por otras incógnitas, y hoy es bien conocido. El ilustre Lagrange trató el problema de una manera un tanto diferente. Como él mismo observó, es claro a partir de la teoría de las fracciones continuas que si la fracción $\frac{a}{b}$ se convierte en la fracción continua

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \text{ etc.}}}} \qquad \pm \cfrac{1}{\mu + \cfrac{1}{n}}$$

donde se toma el signo superior cuando el número de términos α, β, γ, $\ldots \lambda$, μ es par, y el inferior cuando es impar.

2º. El orden de los números α, β, γ, etc. puede invertirse: $[\alpha, \beta, \gamma, \ldots, \lambda, \mu] = [\mu, \lambda, \ldots, \gamma, \beta, \alpha]$. Omitimos las demostraciones sencillas.

y si de la última parte se borra $\frac{1}{n}$ y se reconvierte en una fracción $\frac{x}{y}$, entonces $ax = by \pm 1$, siempre que a sea primo a b. Además, se obtiene el mismo algoritmo de los dos métodos. Las investigaciones del ilustre Lagrange aparecen en *Hist. de l'Ac. de Berlin*, 1767, *p.* 173, y con otros en los apéndices de la versión francesa del *Algebra* de Euler.

29.

La congruencia $ax + t \equiv u$, cuyo módulo no es primo a a, se reduce fácilmente al caso anterior. Sea m el módulo y sea δ el máximo común divisor de a y m. Es claro que cualquier valor de x que satisface la congruencia según el módulo m también la satisface según el módulo δ (art. 5). Pero $ax \equiv 0 \pmod{\delta}$ puesto que δ divide a a. Por tanto la congruencia no tiene solución a menos que $t \equiv u \pmod{\delta}$, esto es $t - u$ es divisible por δ.

Ahora, sean $a = \delta e$, $m = \delta f$, $t - u = \delta k$; e será primo a f. Entonces $ex + k \equiv 0 \pmod{f}$ será equivalente a la congruencia propuesta $ax + t \equiv u$; esto es, cualquier valor de x que cumple la una también satisfará la otra y viceversa. Porque claramente $ex + k$ es divisible por f cuando $\delta ex + \delta k$ es divisible por δf, y viceversa. Pero vimos antes cómo resolver la congruencia $ex + k \equiv 0 \pmod{f}$; así es claro que si v es uno de los valores de x, $x \equiv v \pmod{f}$ nos da la solución completa de la congruencia propuesta.

30.

Cuando el módulo es compuesto, a veces es ventajoso usar el siguiente método.

Sea el módulo $= mn$, y la congruencia propuesta $ax \equiv b$. Primero, se resuelve la congruencia según el módulo m, y se supone que resulta $x \equiv v \pmod{\frac{m}{\delta}}$ donde δ es el máximo común divisor de los números m y a. Es claro que cualquier valor de x que satisface la congruencia $ax \equiv b$ según el módulo mn también la satisface según el módulo m, y será expresable en la forma $v + \frac{m}{\delta}x'$ donde x' es algún número indeterminado. El recíproco, sin embargo, no es cierto puesto que no todos los números de la forma $v + \frac{m}{\delta}x'$ satisfacen la congruencia según el módulo mn. La manera de determinar x' tal que $v + \frac{m}{\delta}x'$ es una raíz de la congruencia $ax \equiv b \pmod{mn}$ puede deducirse de la solución de la congruencia $\frac{am}{\delta}x' + av \equiv b \pmod{mn}$ o de la congruencia equivalente $\frac{a}{\delta}x' \equiv \frac{b-av}{m} \pmod{n}$. Por tanto la resolución de cualquier congruencia según el módulo mn puede reducirse a la resolución de dos

congruencias según los módulos m y n. Y es evidente que si n es otra vez el producto de dos factores, la resolución de la congruencia, relativa al módulo n depende de la resolución de las congruencias cuyos módulos son estos factores. En general la resolución de una congruencia según el módulo compuesto depende de la resolución de otras congruencias cuyos módulos son factores del módulo compuesto. Estos factores pueden tomarse como números primos si esto es conveniente.

Ejemplo. Si se propone la congruencia $19x \equiv 1 \pmod{140}$, se resuelve primero según el módulo 2, y resulta $x \equiv 1 \pmod{2}$. Sea $x = 1+2x'$; se convierte en $38x' \equiv -18 \pmod{140}$, o lo que es equivalente, $19x' \equiv -9 \pmod{70}$. Si se resuelve esta otra vez según el módulo 2, resulta $x' \equiv 1 \pmod{2}$, y al colocar $x' = 1 + 2x''$ se convierte en $38x'' \equiv -28 \pmod{70}$ o $19x'' \equiv -14 \pmod{35}$. Según el módulo 5 nos da la solución $x'' \equiv 4 \pmod{5}$, y sustituyendo $x'' = 4 + 5x'''$ se convierte en $95x''' \equiv -90 \pmod{35}$ o $19x''' \equiv -18 \pmod{7}$. De esto resulta $x''' \equiv 2 \pmod{7}$, y al colocar $x''' = 2 + 7x''''$ resulta $x = 59 + 140x''''$; por lo tanto $x \equiv 59 \pmod{140}$ es la solución completa de la congruencia propuesta.

31.

De la misma manera que se expresa la raíz de la ecuación $ax = b$ por $\frac{b}{a}$, designamos por $\frac{b}{a}$ la raíz de la congruencia $ax \equiv b$, y adjuntamos el módulo de la congruencia para distinguirla. Así por ejemplo, $\frac{19}{17} \pmod{12}$ significa cualquier número que es $\equiv 11 \pmod{12}$*). Es claro de esto en general que $\frac{b}{a} \pmod{c}$ no significa nada real (o si se quiere, es imaginario) cuando a y c tienen un común divisor que no divide a b. Aparte de este caso excepcional, la expresión $\frac{b}{a} \pmod{c}$ siempre tendrá valores reales, de hecho, un número infinito de ellos. Todos ellos serán congruentes según c cuando a es primo a c, o primo a $\frac{c}{\delta}$ cuando δ es el máximo común divisor de c y a.

Estas expresiones tienen un algoritmo muy parecido al empleado para las fracciones ordinarias. Indicamos unas propiedades que pueden deducirse fácilmente de la discusión anterior.

1. Si según el módulo c, $a \equiv \alpha$, $b \equiv \beta$, entonces las expresiones $\frac{a}{b} \pmod{c}$ y $\frac{\alpha}{\beta} \pmod{c}$ son equivalentes.
2. $\frac{a\delta}{b\delta} \pmod{c\delta}$ y $\frac{a}{b} \pmod{c}$ son equivalentes.
3. $\frac{ak}{bk} \pmod{c}$ y $\frac{a}{b} \pmod{c}$ son equivalentes cuando k es primo a c.

*) Por analogía esto puede expresarse como $\frac{11}{1} \pmod{12}$.

Podríamos citar muchas otras proposiciones parecidas, pero, como no presentan ninguna dificultad ni son necesarias para lo siguiente, procedemos a otros temas.

La búsqueda de un número congruente a un número dado según un módulo dado.

32.

Se puede fácilmente, por medio de lo que precede, *hallar todos los números que tienen residuos dados, según cualquier módulo,* esto nos servirá mucho en lo que sigue.

Sean, en primer lugar, A y B, dos módulos según los cuales el número buscado z tiene que ser congruente a los números a y b. Todos los valores de z están necesariamente contenidos en la fórmula $Ax + a$, donde x es indeterminado, pero tal que $Ax + a \equiv b \pmod{B}$. De manera que si δ es el máximo común divisor de A y de B, la resolución completa de esta congruencia tomará la forma $x \equiv v \pmod{\frac{B}{\delta}}$, o sea, lo que es igual, $x = v + \frac{kB}{\delta}$, siendo k un número entero indeterminado. Por lo tanto, la fórmula $Av + a + \frac{kAB}{\delta}$ contiene todos los valores de z, lo que se reduce a $z \equiv Av + a \pmod{\frac{AB}{\delta}}$. Si hay un tercer módulo C según el cual el número buscado tiene que ser congruente a c, se sigue el mismo procedimiento, según el cual se debe reunir las dos primeras condiciones en una sola. Así, sea ϵ el máximo común divisor de los números $\frac{AB}{\delta}$ y C, entonces se obtendrá la congruencia $\frac{AB}{\delta}x + Av + a \equiv c \pmod{C}$, que será resuelta por una congruencia de la forma $x \equiv w \pmod{\frac{C}{\epsilon}}$ y la propuesta será resuelta completamente por la congruencia $z \equiv \frac{ABw}{\delta} + Av + a \pmod{\frac{ABC}{\delta\epsilon}}$. Se procede de la misma manera sea cual sea el número de módulos. Es conveniente observar que $\frac{AB}{\delta}$ y $\frac{ABC}{\delta\epsilon}$ son los menores números divisibles a la vez por A y B, o por A, B y C y se puede concluir fácilmente que sea cual sea la cantidad de módulos A, B, C, etc., si se representa por M el menor número divisible por cada uno de ellos, se tendrá la resolución completa al tomar $z \equiv r \pmod{M}$. Pero cuando alguna de las congruencias auxiliares es irresoluble, concluimos que el problema involucra una imposibilidad. Pero obviamente esto no puede ocurrir cuando todos los números A, B, C, etc., son primos entre sí.

Ejemplo. Sean los números A, B, C, a, b, c, iguales a 504, 35, 16, 17, -4, 33. Aquí las dos condiciones $z \equiv 17 \pmod{504}$ y $z \equiv -4 \pmod{35}$ son equivalentes a la única condición $z \equiv 521 \pmod{2520}$. Al adjuntar la condición $z \equiv 33 \pmod{16}$, nos dará finalmente $z \equiv 3041 \pmod{5040}$.

33.

Si todos los números A, B, C, etc., son primos entre sí, es claro que el producto de ellos es igual a su mínimo común múltiplo. En tal caso, todas las congruencias $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, etc., son equivalentes a la única congruencia $z \equiv r \pmod{R}$, donde R denota el producto de los números A, B, C, etc. Resulta en seguida que la sola condición $z \equiv r \pmod{R}$, puede descomponerse en varias; de hecho, si R se resuelve en factores A, B, C, etc., que son primos entre sí, entonces las condiciones $z \equiv r \pmod{A}$, $z \equiv r \pmod{B}$, $z \equiv r \pmod{C}$ etc., agotan la condición original. Esta observación nos abre no solamente un método de descubrimiento de la imposibilidad cuando existe, sino también un método más cómodo y más elegante para calcular las raíces.

34.

Sean, como arriba, $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, $z \equiv c \pmod{C}$. Se resuelven todos los módulos en factores que son primos entre sí: A en A', A'', A''', etc., B en B', B'', B''', etc., y de tal manera que los números A', A'', etc., B', B'', etc., etc., o bien son primos o bien son potencias de primos. Si cualquiera de los números A, B, C, etc., ya es primo o la potencia de un primo, no hay que resolverlo en factores. Entonces, de lo anterior es claro que en vez de las condiciones propuestas podemos poner las siguientes: $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, $z \equiv a \pmod{A'''}$, etc., $z \equiv b \pmod{B'}$, $z \equiv b \pmod{B''}$, etc., etc. Ahora, si no todos los números A, B, C, son primos entre sí (por ejemplo si A no es primo a B), es obvio que no pueden ser diferentes todos los factores primos de A y B. Tiene que ser uno u otro de ellos entre los factores A', A'', A''', etc., que tiene entre los factores B', B'', B''', etc., uno que es igual, o bien un múltiplo, o bien un divisor propio. Primero, supóngase que $A' = B'$. Entonces las condiciones $z \equiv a \pmod{A'}$, $z \equiv b \pmod{B'}$, tienen que ser idénticas; $a \equiv b \pmod{A' \text{ o } B'}$, y así se puede ignorar una. Sin embargo, si no se da que $a \equiv b \pmod{A}$, el problema es imposible de resolver. Si, en segundo lugar, B' es múltiplo de A', la condición $z \equiv a \pmod{A'}$ tiene que ser incluída en la condición $z \equiv b \pmod{B'}$; o sea la congruencia $z \equiv b \pmod{A'}$ que se deduce de la posterior tiene que ser idéntica a la primera. De esto se sigue que la condición $z \equiv a \pmod{A}$ puede rechazarse a menos que sea inconsistente con alguna otra condición (en cuyo caso el problema es imposible). Cuando todas las condiciones superfluas han sido rechazadas, todos los módulos que queden de los factores A', A'', A''', etc., B', B'', B''', etc., etc. serán primos entre sí. Entonces podemos estar seguros de la

posibilidad del problema y proceder como antes.

35.

Ejemplo. Si, como arriba (art. 32), $z \equiv 17 \pmod{504}$, $z \equiv -4 \pmod{35}$ y $z \equiv 33 \pmod{16}$, entonces estas condiciones pueden reducirse a las siguientes: $z \equiv 17 \pmod{8}$, $\equiv 17 \pmod{9}$, $\equiv 17 \pmod{7}$, $\equiv -4 \pmod{5}$, $\equiv -4 \pmod{7}$, $\equiv 33 \pmod{16}$. De estas condiciones $z \equiv 17 \pmod{8}$, $z \equiv 17 \pmod{7}$, pueden omitirse puesto que la primera está contenida en la condición $z \equiv 33 \pmod{16}$ y la segunda es idéntica a $z \equiv -4 \pmod{7}$. Permanecen:

$$z \equiv \left| \begin{array}{l} 17 \pmod{9} \\ -4 \pmod{5} \\ -4 \pmod{7} \\ 33 \pmod{16} \end{array} \right. \qquad \text{y así:} \quad z \equiv 3041 \pmod{5040}$$

Es cierto que a veces es más conveniente reunir las congruencias que se derivan de una misma condición separadamente de las condiciones restantes, puesto que es fácil hacerlo; e.g., cuando se eliminan unas de las condiciones $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, etc., se reemplazan las restantes por $z \equiv a$ según el módulo que es el producto de todos los módulos que se quedan del conjunto A', A'', A''', etc. Así que, en nuestro ejemplo, las condiciones $z \equiv -4 \pmod{5}$, $z \equiv -4 \pmod{7}$ se reemplazan por $z \equiv -4 \pmod{35}$. Además resulta que no es indiferente para abreviar los cálculos cuáles condiciones superfluas se rechazan. Pero no es nuestro propósito tratar estos detalles ni otros artificios prácticos que pueden aprenderse más fácilmente por práctica que por preceptos.

36.

Cuando todos los módulos A, B, C, D, etc., son primos entre sí, muchas veces es mejor usar el siguiente método.

Se determina un número congruente a la unidad según el módulo A, y congruente a 0 según el producto de los módulos restantes; o sea, será un valor (preferiblemente el menor) de la expresión $\frac{1}{BCD \text{ etc.}} \pmod{A}$ multiplicado por BCD etc. (véase art. 32). De manera semejante, sea $\beta \equiv 1 \pmod{B}$ y $\equiv 0 \pmod{ACD \text{ etc.}}$, $\gamma \equiv 1 \pmod{C}$ y $\equiv 0 \pmod{ABD \text{ etc.}}$, etc. Entonces si se

desea un número z que según los módulos A, B, C, D, etc., sea congruente a a, b, c, d, etc., respectivamente, podemos colocar:

$$z \equiv \alpha a + \beta b + \gamma c + \delta d \text{ etc. } (\text{mod. } ABCD \text{ etc.})$$

Es obvio que $\alpha a \equiv a \pmod{A}$ y que todos los restantes números βb, γc, etc. son todos $\equiv 0 \pmod{A}$, así que $z \equiv a \pmod{A}$. Una demostración semejante vale para los otros módulos. Esta solución es preferible a la primera cuando tenemos que resolver más problemas del mismo tipo para los cuales los módulos A, B, C, etc., mantienen sus valores, puesto que así α, β, γ, etc., tienen valores constantes. Esto ocurre en el problema de la cronología donde se intenta determinar el año juliano dados su número dorado y su ciclo solar. Aquí $A = 15$, $B = 19$, $C = 28$, así que el valor de la expresión $\frac{1}{19 \cdot 28} \pmod{15}$, o $\frac{1}{532} \pmod{15}$ es 13, luego $\alpha = 6916$. De manera que β es 4200 y γ es 4845, así que el número que deseamos es el menor residuo del número $6916a + 4200b + 4845c$, donde a es la indicción, b el número dorado, c el ciclo solar.

Congruencias lineales con varias incógnitas.

37.

Esto basta para las congruencias del primer grado con una incógnita. Se procede a las congruencias que contienen varias incógnitas. Si expusiéramos el asunto con todo rigor, esta sección nunca terminaría. Por tanto, se propone tratar solamente lo que parezca merecer atención, restringir nuestra investigación a unas observaciones, y dejar una exposición completa para otra ocasión.

1) Al igual que en las ecuaciones, vemos que se debe tener tantas congruencias como incógnitas por determinar.

2) Se proponen, entonces, las congruencias

$$ax + by + cz + \cdots \equiv f \pmod{m} \qquad (A)$$
$$a'x + b'y + c'z + \cdots \equiv f' \qquad (A')$$
$$a''x + b''y + c''z + \cdots \equiv f'' \qquad (A'')$$
$$\text{etc.}$$

de las cuales hay tantas como incógnitas x, y, z, etc.

Ahora, se determinan los números ξ, ξ', ξ'', etc., tales que

$$\begin{gathered} b\xi + b'\xi' + b''\xi'' + \text{ etc.} = 0 \\ c\xi + c'\xi' + c''\xi'' + \text{ etc.} = 0 \\ \text{etc.} \end{gathered}$$

y tales que todos los números sean enteros sin común divisor, lo cual es siempre posible por la teoría de las ecuaciones lineales. De modo semejante ν, ν', ν'', etc., ζ, ζ', ζ'', etc., etc., tales que

$$\begin{gathered} a\nu + a'\nu' + a''\nu'' + \text{ etc.} = 0 \\ c\nu + c'\nu' + c''\nu'' + \text{ etc.} = 0 \\ \text{etc.} \\ a\zeta + a'\zeta' + a''\zeta'' + \text{ etc.} = 0 \\ b\zeta + b'\zeta' + b''\zeta'' + \text{ etc.} = 0 \\ \text{etc.} \quad \text{etc.} \end{gathered}$$

3) Es claro que si se multiplican las congruencias A, A', A'', etc., por ξ, ξ', ξ'', etc., luego por ν, ν', ν'', etc., etc., y luego se suman, resultarán las siguientes congruencias:

$$\begin{gathered} (a\xi + a'\xi' + a''\xi'' + \text{ etc.})x \equiv f\xi + f'\xi' + f''\xi'' + \text{ etc.} \\ (b\nu + b'\nu' + b''\nu'' + \text{ etc.})y \equiv f\nu + f'\nu' + f''\nu'' + \text{ etc.} \\ (c\zeta + c'\zeta' + c''\zeta'' + \text{ etc.})z \equiv f\zeta + f'\zeta' + f''\zeta'' + \text{ etc.} \\ \text{etc.} \end{gathered}$$

las cuales escribimos por brevedad de la manera siguiente:

$$\sum(a\xi)x \equiv \sum(f\xi), \quad \sum(b\nu)y \equiv \sum(f\nu), \quad \sum(c\zeta)z \equiv \sum(f\zeta), \quad \text{etc.}$$

4) Ahora se distinguen varios casos.

Primero, cuando todos los coeficientes $\sum(a\xi)$, $\sum(b\nu)$, etc. son primos a m, el módulo de las congruencias, ellas se resuelven según los preceptos ya tratados, y se

encuentra la solución completa por congruencias de la forma $x \equiv p \pmod{m}$, $y \equiv q \pmod{m}$, etc.*) E.g., si se proponen las congruencias

$$x + 3y + z \equiv 1, \quad 4x + y + 5z \equiv 7, \quad 2x + 2y + z \equiv 3 \pmod{8}$$

se encuentra que $\xi = 9$, $\xi' = 1$, $\xi'' = -14$, luego $-15x \equiv -26$ luego $x \equiv 6 \pmod{8}$. De igual manera se encuentra que $15y \equiv -4$, $15z \equiv 1$, y así que $y \equiv 4$, $z \equiv 7 \pmod{8}$.

5) *Segundo,* cuando no todos los coeficientes $\sum(a\xi)$, $\sum(b\nu)$, etc., son primos al módulo, sean α, β, γ, etc., los máximos comunes divisores del módulo m con $\sum(a\xi)$, $\sum(b\nu)$, $\sum(c\zeta)$, etc. respectivamente. Es claro que el problema es imposible a menos que ellos dividan los números $\sum(f\xi)$, $\sum(f\nu)$, $\sum(f\zeta)$, etc., respectivamente. Sin embargo, cuando se cumplan estas condiciones, es claro que las congruencias en (3) se resolverán completamente por congruencias de la forma $x \equiv p \pmod{\frac{m}{\alpha}}$, $y \equiv q \pmod{\frac{m}{\delta}}$, $z \equiv r \pmod{\frac{m}{\gamma}}$, etc., o si se quiere hay α valores diferentes de x (o sea, no congruentes según m), digamos p, $p + \frac{m}{\alpha}, \ldots p + \frac{(\alpha-1)m}{\alpha}$, β valores diferentes de y, etc., que satisfacen las congruencias. Es evidente que todas las soluciones de las congruencias propuestas (si hay) se encuentran entre éstas. Pero esta solución no puede invertirse puesto que en general no todas las combinaciones de todos los valores de x, al combinarlos con todos los de y y z etc., satisfacen el problema, sino únicamente aquéllas cuya interrelación puede mostrarse por una o varias de las congruencias condicionales. Sin embargo, como la solución completa de este problema no es necesaria para lo que sigue, no desarrollaremos el argumento más sino que ilustraremos la idea por medio de un ejemplo.

Sean las congruencias propuestas:

$$3x + 5y + z \equiv 4, \quad 2x + 3y + 2z \equiv 7, \quad 5x + y + 3z \equiv 6 \pmod{12}$$

Entonces, ξ, ξ', ξ''; ν, ν', ν''; ζ, ζ', ζ'' serán respectivamente iguales a 1, -2, 1; 1, 1, -1; -13, 22, -1, y de esto $4x \equiv -4$, $7y \equiv 5$, $28z \equiv 96$. A partir de esto se crean cuatro valores de x, digamos $\equiv 2, 5, 8, 11$; un valor de y, digamos $\equiv 11$, y cuatro valores de z, digamos $\equiv 0, 3, 6, 9 \pmod{12}$. Ahora, para saber cuáles

*) Esta conclusión requiere demostración, pero la hemos suprimido aquí. Nada más resulta de nuestro análisis que las congruencias propuestas no pueden resolverse por otros valores de las incógnitas x, y, etc. No hemos mostrado que estos valores de hecho la satisfacen. Aún es posible que no haya ninguna solución. Un paralelismo ocurre en el tratamiento de las ecuaciones lineales.

combinaciones de los valores de x pueden usarse con los valores de z, se sustituyen en las congruencias propuestas para x, y, z, respectivamente, $2 + 3t$, 11, $3u$. Esto convierte las congruencias en

$$57 + 9t + 3u \equiv 0, \quad 30 + 6t + 6u \equiv 0, \quad 15 + 15t + 9u \equiv 0 \pmod{12},$$

y fácilmente se ven equivalentes a

$$19 + 3t + u \equiv 0, \quad 10 + 2t + 2u \equiv 0, \quad 5 + 5t + 3u \equiv 0 \pmod{4}.$$

La primera claramente requiere que $u \equiv t + 1 \pmod{4}$; al sustituir este valor en las restantes congruencias, también las satisface. Se concluye que los valores 2, 5, 8, 11 de x, que resultan al poner $t \equiv 0, 1, 2, 3$, están necesariamente combinados con los valores de $z \equiv 3, 6, 9, 0$, respectivamente. En total tenemos cuatro soluciones:

$$\begin{aligned} x &\equiv \quad 2, \quad 5, \quad 8, 11 \pmod{12} \\ y &\equiv 11, 11, 11, 11 \\ z &\equiv \quad 3, \quad 6, \quad 9, \quad 0 \end{aligned}$$

A estas investigaciones, las cuales completan la finalidad que habíamos propuesto para esta sección, adjuntamos unas cuantas proposiciones que dependen de los mismos principios y que serán útiles frecuentemente en lo que sigue.

Varios Teoremas.

38.

PROBLEMA. *Hallar cuántos números positivos hay menores que un número positivo dado A, y a la vez primos a él.*

Por brevedad simbolizamos el número de enteros positivos que son primos a A y menores que él por el prefijo φ. Por lo tanto se busca a φA.

I. Cuando A *es primo,* es claro que todos los números desde 1 hasta $A - 1$ son primos a A; y así en este caso resultará

$$\varphi A = A - 1$$

II. Cuando A *es la potencia de un primo,* digamos $= p^m$, ninguno de los números divisibles por p será primo a A, pero los demás sí. Entonces, de los $p^m - 1$

números, tienen que rechazarse: p, $2p$, $3p$, $\ldots$, $(p^{m-1}-1)p$. Por lo tanto sobran $p^m - 1 - (p^{m-1}-1)$ o sea $p^{m-1}(p-1)$ de ellos. Así

$$\varphi p^m = p^{m-1}(p-1)$$

III. Los casos restantes se reducen fácilmente a estos mediante la siguiente proposición: *Si A se resuelve en factores M, N, P, etc., que son primos entre sí, será*

$$\varphi A = \varphi M \cdot \varphi N \cdot \varphi P \text{ etc.}$$

Esto se demuestra como sigue. Sean m, m', m'', etc., los números primos a M y menores que M, y sea el número de ellos $= \varphi M$. De manera semejante, sean n, n', n'', etc., p, p', p'', etc., los números primos a N y a P, respectivamente y menores que ellos, y sean φN, φP, etc., los números de ellos. Es evidente que todos los números que son primos al producto A, también serán primos a los factores individuales M, N, P, etc., y viceversa (art. 19); y además que todos los números congruentes a cualquiera de m, m', m'', etc., serán primos a M y viceversa. De modo semejante para N, P, etc. Así el problema se reduce a éste: determinar cuántos números hay menores que A y también congruentes según el módulo M a los números m, m', m'', etc., y que son congruentes según el módulo N a los números n, n', n'', etc. Pero del artículo 32 se sigue que todos los números que tienen residuos dados según cada uno de los módulos M, N, P, etc., serán congruentes según su producto A. Así habrá únicamente uno que es menor que A y congruente a los residuos dados según M, N, P, etc. Por lo tanto, el número que buscamos es igual al número de combinaciones de cada uno de los números m, m', m'', etc., con cada uno de los n, n', n'', etc., y p, p', p'', etc., etc. Es evidente que por la teoría de las combinaciones esto será $= \varphi M \cdot \varphi N \cdot \varphi P$ etc. *Q. E. D.*

IV. Ahora es fácil ver cómo aplicar esto al caso considerado. Sea A resuelto en sus factores primos; esto es, reducido a la forma $a^\alpha b^\beta c^\gamma$ etc., donde a, b, c, etc., son números primos diferentes. Entonces se tendrá

$$\varphi A = \varphi a^\alpha \cdot \varphi b^\beta \cdot \varphi c^\gamma \text{ etc.} = a^{\alpha-1}(a-1)b^{\beta-1}(b-1)c^{\gamma-1}(c-1) \text{ etc.}$$

o, con más elegancia,

$$\varphi A = A \cdot \frac{a-1}{a} \cdot \frac{b-1}{b} \cdot \frac{c-1}{c} \text{ etc.}$$

Ejemplo. Sea $A = 60 = 2^2 \cdot 3 \cdot 5$; entonces $\varphi A = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot 60 = 16$. Los números que son primos a 60 son 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

La primera resolución de este problema aparece en la memoria del ilustre Euler titulada *Theoremata arithmetica nova methodo demostrata* (Comm. nov. Ac. Petrop. VIII p. 74). La demostración se repitió en otra disertación titulada *Speculationes circa quasdam insignes propietates numerorum* (Acta Petrop. VIII, p. 17).

39.

Si determinamos el significado del símbolo φ de tal manera que φA exprese el número de enteros que son primos a A y *no mayores* que A, es evidente que ya no vale $\varphi 1 = 0$ sino $= 1$. No se cambia nada en ningún otro caso. Tomando esta definición, tendremos el teorema siguiente:

Si a, a', a'', etc. son todos los divisores de A (incluyendo a 1 y a A mismo), se tendrá

$$\varphi a + \varphi a' + \varphi a'' + \text{ etc.} = A$$

Ejemplo. Si $A = 30$, entonces $\varphi 1 + \varphi 2 + \varphi 3 + \varphi 5 + \varphi 6 + \varphi 10 + \varphi 15 + \varphi 30 = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$

Demostración. Se multiplican por $\frac{A}{a}$ todos los números que sean primos a a y no mayores que a, por $\frac{A}{a'}$ todos los números primos a a' y no mayores que a', etc., y se tendrán $\varphi a + \varphi a' + \varphi a'' +$ etc. números, ninguno mayor que A mismo. Pero:

1) Todos estos números serán diferentes. De hecho, es evidente que todos aquéllos engendrados por un mismo divisor de A serán diferentes. Ahora, si dos números diferentes fueran engendrados por dos divisores diferentes M y N, y por dos números μ y ν que fueran primos respectivamente a M y N, esto es, si $(\frac{A}{M})\mu = (\frac{A}{N})\nu$, resultaría que $\mu N = \nu M$. Supóngase que $M > N$ (lo cual se puede). Como M es primo a μ , y como divide al número μN, tiene que dividir a N. Por lo tanto, un número mayor divide a un número menor. *Q. E. A.*

2) Se incluyen todos los números 1, 2, 3, $\ldots A$, entre estos números. Sea t un número cualquiera no mayor que A, y sea δ el máximo común divisor de A y t. $\frac{A}{\delta}$ será el divisor de A que es primo a $\frac{t}{\delta}$. Es evidente que este número se encuentra entre los engendrados por el divisor $\frac{A}{\delta}$.

3) Resulta de esto que el número de estos enteros será A y por lo tanto

$$\varphi a + \varphi a' + \varphi a'' + \text{ etc.} = A. \quad Q.\ E.\ D.$$

40.

Si el máximo común divisor de los números A, B, C, D, etc. $= \mu$, siempre pueden determinarse números a, b, c, d, etc., tal que

$$aA + bB + cC + \text{ etc.} = \mu.$$

Demostración. Consideramos primero dos de tales números A y B, y sea su máximo común divisor $= \lambda$. Entonces, la congruencia $Ax \equiv \lambda \pmod{B}$ será resoluble (art. 30). Sea la raíz $= \alpha$, y se pone $\frac{\lambda - A\alpha}{B} = \beta$. Entonces se obtendrá $\alpha A + \beta B = \lambda$ como deseamos.

Si hay un tercer número C, sea λ' el máximo común divisor de los números λ y C, el cual será también el máximo común divisor de los números A, B y C*). Determínense números k y γ tales que $k\lambda + \gamma C = \lambda'$, entonces $k\alpha A + k\beta B + \gamma C = \lambda'$.

Si hay un cuarto número D, sea λ'' el máximo común divisor de los números λ' y D (es fácil ver que será también el máximo común divisor de A, B, C y D), y sea $k'\lambda' + \delta D = \lambda''$. Entonces tenemos $kk'\alpha A + kk'\beta B + k'\gamma C + \delta D = \lambda''$.

De manera semejante se procede si todavía hay más números.

Y si los números A, B, C, D, etc., no tienen divisor común, claramente se tiene

$$aA + bB + cC + \text{ etc.} = 1$$

41.

Si p es número primo y se tienen p objetos, entre los que cualquier número de ellos pueden ser iguales, pero no todos, el número de permutaciones de estos objetos será divisible por p.

---

*) Obviamente λ' divide a todos los números A, B y C. Si no fuera el *máximo* común divisor, el máximo sería mayor que λ'. Ahora, puesto que este máximo divisor divide a A, B y C, también divide a $k\alpha A + k\beta B + \gamma C$, es decir, a λ' mismo. Así un número grande divide a uno pequeño Q. E. A. Este resultado puede ser aún más fácilmente establecido del art. 18.

Ejemplo. Cinco objetos A, A, A, B, B pueden disponerse de diez maneras diferentes.

La demostración de este teorema puede derivarse fácilmente de la conocida teoría de permutaciones. Supóngase que entre estos objetos hay a iguales a A, B iguales a B, c iguales a C, etc. (cualesquiera de a, b, c, etc. pueden ser iguales a la unidad), entonces se tiene

$$a + b + c + \text{ etc.} = p$$

y el número de permutaciones será

$$\frac{1 \cdot 2 \cdot 3 \cdots p}{1 \cdot 2 \cdot 3 \cdots a \cdot 1 \cdot 2 \cdots b \cdot 1 \cdot 2 \cdots c \text{ etc.}}$$

Ahora, es claro que el numerador tiene que ser divisible por el denominador, puesto que el número de permutaciones debe ser un entero. Pero el numerador es divisible por p, mientras que el denominador, el cual está compuesto de factores menores que p, no es divisible por p (art. 15). Así el número de permutaciones será divisible por p (art. 19).

Esperamos que la siguiente demostración complacerá al lector.

Cuando en dos permutaciones de los mismos objetos el orden de ellas no difiere salvo que el primero en una ocupa una posición diferente en la otra mientras que los restantes siguen el mismo orden, de manera que, en el segundo orden, el primer objeto del primer orden sigue al último de él, las llamamos: *permutaciones semejantes**). Así, en nuestro ejemplo, las permutaciones $ABAAB$ y $ABABA$ serán semejante puesto que los objetos que ocupan los lugares primero, segundo, etc., según la primera, ocuparán los lugares tercero, cuarto, etc., en la última, siguiendo la misma sucesión.

Ahora, como cualquier permutación está compuesta de p objetos, es evidente que se pueden encontrar $p - 1$ permutaciones que sean semejantes a ella avanzando el objeto del primer lugar al segundo, al tercero, etc. Es evidente que el número de todas las permutaciones no idénticas es divisible por p puesto que este número es p veces mayor que el número de todas las permutaciones no semejantes.

Supongamos, pues, que dos permutaciones

$$PQ \ldots TV \ldots YZ; \quad V \ldots YZPQ \ldots T,$$

*) Si se conciben las permutaciones semejantes como escritas sobre una circunferencia, de modo que la última sea contigua a la primera, no habrá ninguna discrepancia puesto que ningún lugar puede llamarse primero o último.

donde se engendra una a partir de la otra avanzando sus términos, sean idénticas, o sea $P = V$, etc. Sea el término P, que es el primero en la primera, el $(n+1)$-ésimo en la siguiente. Entonces, en la sucesión siguiente el $(n+1)$-ésimo término será igual al primero, el $(n+2)$-ésimo al segundo, etc., y el $(2n+1)$-ésimo vuelve a ser igual al primero, como el $(3n+1)$-ésimo, etc.; y , en general, el $(kn+m)$-ésimo término igual al m-ésimo (donde, cuando $kn+m$ supera a p mismo, es necesario concebir la sucesión $V \ldots YZPQ \ldots T$ como repetida contínuamente desde el comienzo, o se resta de $kn+m$ el múltiplo de p menor que $kn+m$ y más próximo en magnitud). Así pues, si se determina k tal que $kn \equiv 1 \pmod{p}$, lo cual siempre puede hacerse, pues p es primo, resulta en general que el m-ésimo término es igual al $(m+1)$-ésimo, o que cada término es igual a su sucesor, i.e., todos los términos son iguales, contrariamente a la hipótesis.

42.

Si los coeficientes A, B, C, ..., N; a, b, c, ..., n de dos funciones de la forma

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \cdots + N \qquad (P)$$
$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} + \cdots + n \qquad (Q)$$

son todos racionales, y no todos enteros, y si el producto de (P) *y* (Q)

$$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{ etc. } + \mathfrak{Z}$$

entonces no todos los coeficientes $\mathfrak{A}$, $\mathfrak{B}$, $\ldots \mathfrak{Z}$ *pueden ser enteros.*

Demostración. Se expresan todos las fracciones entre los coeficientes A, B, etc., a, b, etc., en su forma reducida, y se elige libremente un primo p que divida uno o varios de los denominadores de estas fracciones. Supongamos que p divide al denominador de uno de los coeficientes en (P). Es claro que si se divide (Q) por p, por lo menos uno de los coeficientes fraccionales en $\frac{(Q)}{p}$ tendrá a p como factor de su denominador (por ejemplo, el primer coeficiente, $\frac{1}{p}$). Ahora, es fácil ver en (P) que siempre habrá un término, una fracción, cuyo denominador involucra potencias *más altas* de p que los denominadores de todos los coeficientes fraccionales que lo preceden y *ninguna* potencia *menor* que los denominadores de todos los coeficientes fraccionales subsiguientes. Sea este término $= Gx^g$, y sea la potencia de p en el denominador

de G, $= t$. Un término semejante puede encontrarse en $\frac{(Q)}{p}$. Sea $= \Gamma x^{\gamma}$, y sea la potencia de p en el denominador de Γ, $= \tau$. Es evidente que $t + \tau$ será $= 2$ por lo menos. Ahora se demostrará que el término $x^{g+\gamma}$ en el producto de (P) y (Q) tendrá un coeficiente fraccional cuyo denominador involucrará $t + \tau - 1$ potencias de p.

Sean $'Gx^{g+1}$, $''Gx^{g+2}$, etc., los términos en (P) que preceden a Gx^{g}, y $G'x^{g-1}$, $G''x^{g-2}$, los que le siguen; de manera semejante sean $'\Gamma x^{\gamma+1}$, $''\Gamma x^{\gamma+2}$, etc., los términos que preceden a Γx^{γ}, y los términos que lo siguen serán $\Gamma' x^{\gamma-1}$, $\Gamma'' x^{\gamma-2}$, etc. Es claro que en el producto de (P) y $\frac{(Q)}{p}$ el coeficiente del término $x^{g+\gamma}$ será

$$\begin{aligned} &= G\Gamma + {}'G\Gamma' + {}''G\Gamma'' + \text{ etc.} \\ &\quad + {}'\Gamma G' + {}''\Gamma G'' + \text{ etc.} \end{aligned}$$

La parte $G\Gamma$ será una fracción, y si se expresa en forma reducida, se involucrarán $t+\tau$ potencias de p en el denominador; las partes restantes, si son fracciones, contendrán en sus denominadores menos potencias de p puesto que todos son productos de dos factores de los cuales uno no contiene más que t potencias de p, el otro menos que τ potencias de p; o el otro no tiene más que τ, y el primero menos que t. Así $G\Gamma$ será de la forma $\frac{e}{fp^{t+\tau}}$, mientras que la suma de las restantes de la forma $\frac{e'}{f'p^{t+\tau-\delta}}$, donde δ es positivo y e, f, f' están libres del factor p: por lo cual la suma de todos será

$$= \frac{ef' + e'fp^{\delta}}{ff'p^{t+\tau}}$$

cuyo numerador no es divisible por p. De tal manera el denominador no puede obtener potencias menores que $t + \tau$ por ninguna reducción. Por lo tanto, el coeficiente del término $x^{g+\gamma}$ en el producto de (P) y (Q) será

$$= \frac{ef' + e'fp^{\delta}}{ff'p^{t+\tau-1}},$$

i.e., una fracción cuyo denominador contiene $t + \tau - 1$ potencias de p. *Q. E. D.*

43.

Las congruencias del m-ésimo grado

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \text{ etc.} + Mx + N \equiv 0$$

cuyo módulo es el número primo p que no divide a A, no pueden resolverse más que de m maneras diferentes, o sea, no pueden tener más que m raíces no congruentes según p. (Vea artículos 25 y 26).

Si se asume falso, tendremos congruencias de grados diferentes m, n, etc., con más de m, n, etc. raíces, y si el menor grado es m, todas las congruencias semejantes de menor grado se encuentran en concordancia con nuestro teorema. Como ya hemos demostrado esto para el primer grado (art. 26), es claro que m es $= 2$ o mayor. Por eso la congruencia

$$Ax^m + Bx^{m-1} + \text{ etc.} + Mx + N \equiv 0$$

admite por lo menos $m + 1$ raíces, $x \equiv \alpha$, $x \equiv \beta$, $x \equiv \gamma$, etc., y suponemos (lo que es válido) que α, β, γ, etc., son positivos y menores que p, y que α es el menor de todos. Ahora, en la congruencia propuesta se sustituye x por $y + \alpha$. La congruencia se transforma en

$$A'y^m + B'y^{m-1} + C'y^{m-2} + \cdots + M'y + N' \equiv 0$$

Entonces es evidente que se satisface esta congruencia si se pone $y \equiv 0$, o $\equiv \beta - \alpha$, o $\equiv \gamma - \alpha$, etc. Todas estas raíces serán diferentes, y el número de ellas $= m + 1$. Pero como $y \equiv 0$ es raíz, N' es divisible por p. Así que también la expresión

$$y(A'y^{m-1} + B'y^{m-2} + \text{ etc.} + M') \quad \text{será} \quad \equiv 0 \pmod{p}$$

si se reemplaza y por uno de los m valores $\beta - \alpha$, $\gamma - \alpha$, etc., todos los cuales son > 0 y $< p$. Así, en todos estos casos, también

$$A'y^{m-1} + B'y^{m-2} + \text{ etc.} + M' \quad \text{será} \quad \equiv 0 \pmod{p}$$

i.e., la congruencia

$$A'y^{m-1} + B'y^{m-2} + \text{ etc.} + M' \equiv 0 \qquad \text{(art. 22)}$$

que es de grado $m - 1$, tiene m raíces, contrariamente a nuestro teorema (es evidente que A' será $= A$ y así no divisible por p, como se requiere), pero hemos supuesto que nuestro teorema vale para toda congruencia de grado inferior a m. *Q. E. A.*

44.

Aunque hemos supuesto que el módulo p no divide al coeficiente del término más alto, el teorema no se restringe sólo a este caso. Porque, si el primer coeficiente o cualquiera de los otros, es divisible por p, puede rechazarse sin riesgo, por eso se reduce la congruencia a un grado inferior, para el cual el primer coeficiente ya no sería divisible por p, a menos que todos los coeficientes sean divisibles por p, en cuyo caso la congruencia sería una identidad y la incógnita completamente indeterminada.

Este teorema primero fue propuesto y demostrado por Lagrange (*Mem. de l'Ac. de Berlin*, 1768 *p.* 192). También se encuentra en la memoria de Legendre, *Recherches d'Analyse indéterminée, Hist. de l'Acad. de Paris* 1785 *p.* 466. El gran Euler en *Nov. Comm. Ac. Petr.* XVIII, *p.* 93 demostró que la congruencia $x^n - 1 \equiv 0$ no puede tener más que n raíces diferentes. A pesar de que era un caso particular, el método que usó este gran señor puede adaptarse fácilmente a todas las congruencias. Anteriormente él había resuelto un caso aún más limitado, *Comm. nov. Ac. Petr.* V *p.* 6 , pero este método no puede generalizarse. En la sección VIII demostraremos este teorema por un método todavía diferente; aunque a primera vista parecen diferentes estos métodos, los expertos que quieran compararlos llegarán fácilmente a ver que todos están construidos sobre el mismo principio. Sin embargo, como el teorema considerado aquí no es más que un lema, y como la exposición completa no pertenece a este lugar, no pararemos aquí para tratar los módulos compuestos por separado.

Sección Tercera

SOBRE

RESIDUOS DE LAS POTENCIAS

Los residuos de los términos de una progresión geométrica que comienza desde la unidad constituyen una serie periódica.

45.

TEOREMA. *En toda progresión geométrica 1, a, a^2, a^3, etc., aparte del primer término, se da además otro término a^t, congruente a la unidad, según el módulo p, que es primo a a, cuyo exponente es $t < p$.*

Demostración. Puesto que el módulo p es primo a a, y por lo tanto es primo a cualquier potencia de a, ningún término de la progresión será $\equiv 0 \pmod{p}$, sino que cada uno será congruente a uno de los números 1, 2, 3, $\ldots p-1$. De éstos, hay $p-1$, pues, es evidente que si se considerasen más que $p-1$ términos de la progresión, no todos pueden tener diferentes residuos mínimos. Entonces, entre los términos 1, a, a^2, a^3, $\ldots a^{p-1}$, se encontrarán al menos dos congruentes a un residuo mínimo. Sea pues, $a^m \equiv a^n$ y $m > n$, y al dividir por a^n, resultará $a^{m-n} \equiv 1$ (art. 22), donde $m - n < p$, y > 0. *Q. E. D.*

Ejemplo. En la progresión 2, 4, 8, etc., el primer término que es congruente a la unidad, según el módulo 13, resulta ser $2^{12} = 4096$. Pero, según el módulo 23, en esta progresión es $2^{11} = 2048 \equiv 1$. Igualmente, 15625, la sexta potencia del número 5, es congruente a la unidad, según el módulo 7, la quinta de ella, 3125, según el módulo 11. Por tanto, en unos casos la potencia congruente a la unidad resulta menor que $p - 1$. Pero, en otros, es necesario ascender hasta la $(p-1)$-ésima potencia.

46.

Cuando se continúa una progresión más allá de un término que es congruente a la unidad, se producen nuevamente los mismos residuos que se tienen al principio. Es claro que si $a^t \equiv 1$, se tendrá $a^{t+1} \equiv a$, $a^{t+2} \equiv a^2$, etc., hasta que se encuentre el término a^{2t} cuyo residuo menor otra vez será $\equiv 1$, y el período de los residuos comenzará de nuevo. Se tiene, pues, un período que comprende t residuos, que en cuanto finaliza se vuelve a repetir desde el comienzo; y ningún otro residuo, salvo aquéllos contenidos en este período, puede aparecer en toda la progresión.

En general, será $a^{mt} \equiv 1$, y $a^{mt+n} \equiv a^n$, lo cual en nuestra notación se presenta así:

Si $r \equiv \rho \pmod{t}$, *será* $a^r \equiv a^\rho \pmod{p}$.

47.

De este teorema, se gana un método para encontrar muy fácilmente los residuos de potencias, tan grandes como sean sus exponentes, una vez que se encuentra una potencia congruente a la unidad. Si, por ejemplo, se busca el residuo resultante de la división de la potencia 3^{1000} por 13, será $3^3 \equiv 1 \pmod{13}$, $t = 3$; como $1000 \equiv 1 \pmod{3}$, será $3^{1000} \equiv 3 \pmod{13}$.

48.

Cuando a^t es la menor potencia congruente a la unidad (excepto $a^0 = 1$, tal caso no será tratado aquí), los t términos que constituyen un período de residuos serán todos diferentes, como se puede ver con facilidad de la demostración del art. 45. Entonces, también la proposición del art. 46 puede invertirse; esto es, si $a^m \equiv a^n \pmod{p}$, será $m \equiv n \pmod{t}$. Pues, si m y n fueran incongruentes según el módulo t, sus residuos mínimos μ, ν serían diferentes. Pero, $a^\mu \equiv a^m$ y $a^\nu \equiv a^n$, así pues $a^\mu \equiv a^\nu$, i.e., no todas las potencias menores que a^t son incongruentes, contra la hipótesis.

Si $a^k \equiv 1 \pmod{p}$, entonces será $k \equiv 0 \pmod{t}$, i.e., k será divisible por t.

Hasta aquí hemos hablado de módulos cualesquiera, primos a a. Ahora, trataremos por aparte los módulos que son números absolutamente primos y luego desarrollaremos una investigación más general con esta base.

Se consideran primero los módulos que son números primos.

49.

TEOREMA. *Si p es un número primo que no divide a a, y si a^t es la menor potencia de a congruente a la unidad, según el módulo p, el exponente t será $= p-1$, o será un factor de este número.*

Consúltese los ejemplos del art. 45.

Demostración. Puesto que ya hemos demostrado que t es $= p-1$ o $< p-1$, falta que, en el segundo caso, se demuestre que t siempre es un factor de $p-1$.

I. Reúnanse los menores residuos positivos de todos estos términos 1, a, a^2, $\ldots a^{t-1}$, que se denotarán por α, α', α'', etc., de modo que sea $\alpha = 1$, $\alpha' \equiv a$, $\alpha'' \equiv a^2$, etc. Se ha visto que todos son diferentes; pues, si dos términos a^m y a^n tuvieran el mismo residuo, (al suponer $m > n$) sería $a^{m-n} \equiv 1$, no obstante que $m - n < t$. Q.E.A., puesto que ninguna potencia inferior a a^t es congruente a la unidad (por hipótesis). Además, todos los α, α', α'', etc. están contenidos en la sucesión de números 1, 2, 3, $\ldots p-1$ que, sin embargo, no se agotan pues $t < p-1$. Denotaremos el conjunto de todos α, α', α'', etc. con (A). Por tanto, (A) contiene t términos.

II. Tómese un número cualquiera β entre 1, 2, 3, $\ldots p-1$ que falte en (A) . Multiplíquese β por todos los α, α', α'', etc. Sean β, β', β'', etc. los residuos menores originados de allí cuyo número será t. Pero estos residuos serán diferentes entre sí y además diferentes de α, α', α'', etc. Si la primera aserción fuera falsa, se tendría $\beta a^m \equiv \beta a^n$, dividiendo por β, $a^m \equiv a^n$, contra lo que hemos demostrado. Si la segunda fuera falsa, se tendría $\beta a^m \equiv a^n$. Por tanto, cuando $m < n$, $\beta \equiv a^{n-m}$, i.e., β sería congruente con uno de éstos α, α', α'', etc. contra la hipótesis; cuando vale $m > n$, al multiplicar por a^{t-m}, $\beta a^t \equiv a^{t+n-m}$, o por medio de $a^t \equiv 1$, $\beta \equiv a^{t+n-m}$, lo cual es un absurdo. Denótese el conjunto de todos los β, β', β'', etc., cuyo número $= t$ con (B) y se tiene ya $2t$ números de 1, 2, 3, $\ldots p-1$. Por tanto, y si (A) y (B) comprenden todos estos números, se tiene $\frac{p-1}{2} = t$. Así el teorema se ha demostrado.

III. Si todavía quedan algunos, sea γ uno de ellos. Multiplíquense por él todos α, α', α'', etc. y sean γ, γ', γ'', etc. los residuos mínimos de los productos y denótese el conjunto de todos ellos con (C). Por tanto, (C) comprende t números de 1, 2, 3, $\ldots p-1$, que son todos diferentes entre sí, y diferentes de los contenidos en (A) y (B). Las primeras aserciones se demuestran de igual modo como en el II, la tercera como sigue: si fuera $\gamma a^m \equiv \beta a^n$, sería $\gamma \equiv \beta a^{n-m}$, ó $\equiv \beta a^{t+n-m}$ según que $m < n$ ó $> n$, y en cualquier caso γ sería congruente a un número de (B) contra

la hipótesis. Por tanto, se tienen $3t$ números de 1, 2, 3, $\ldots p-1$ y si no faltan más resulta $t = \frac{p-1}{3}$ y así el teorema quedará demostrado.

IV. Si faltan todavía otros, del mismo se habrá de proceder a un cuarto conjunto (D) de números, etc. Pero, es evidente, puesto que el número de enteros 1, 2, 3, $\ldots p-1$ es finito, que al fin se habrán de agotar todos ellos, y que será un múltiplo de t: por eso t será algún factor del número $p-1$. *Q. E. D.*

El teorema de Fermat.

50.

Así, puesto que $\frac{p-1}{t}$ es un entero, resulta al elevarse ambas partes de la congruencia $a^t \equiv 1$ a la potencia $\frac{p-1}{t}$, $a^{p-1} \equiv 1$ *ó sea* $a^{p-1} - 1$ *siempre es divisible por* p*, cuando* p *es un primo que no divide a* a*.*

Este teorema, el cual ya sea por su elegancia o por su gran utilidad es digno de toda atención, suele llamarse el *teorema de Fermat,* por su inventor. (Véase Fermat, *Opera Matem.*, Toulouse 1679, p. 163). El inventor no presentó una demostración, sin embargo afirmó tener una en su poder. El gran Euler fue el primero que publicó una demostración, en su disertación titulada *Theorematum quorundam ad numeros primos spectantium demonstratio, Comm. Acad. Petrop. T.* VIII.*) Se basa ésta en el desarrollo de la potencia $(a+1)^p$, donde se deduce fácilmente de la forma de los coeficientes, que $(a+1)^p - a^p - 1$ siempre será divisible por p cuando $a^p - a$ es divisible por p. Ahora, como $1^p - 1$ siempre es divisible por p, también $2^p - 2$ lo será siempre, por tanto también $3^p - 3$, y en general $a^p - a$. Y si p no divide a a, tampoco $a^{p-1} - 1$ será divisible por p. Esto basta para aclarar la idea del método. El gran Lambert presentó una demostración parecida en *Actis Erudit,* 1769, p. 109. Porque se veía que el desarrollo de una potencia binomia era bastante ajeno de la teoría de los números, el gran Euler buscó otra demostración que aparece en *Comment. nov. Petr. T.* VII p. 70, y que está en armonía con lo que expusimos en el artículo anterior. Además, en lo siguiente, se nos ofrecerán otras demostraciones. En este lugar, se permite añadir otra más, la cual se basa en principios semejantes a los de la primera del gran Euler.

*) En un comentario anterior, el gran hombre todavía no había logrado su propósito. *Comm. Petr. T.* VI p. 106.— En una controversia famosa entre Maupertuis y König, surgida sobre el principio de la acción mínima, aunque muy pronto llevó a una variedad de cosas, König afirmó tener en su poder una carta de Leibniz, en la cual está contenida una demostración de este teorema que concuerda con la primera de Euler. *Appel au public.* p. 106. No queremos negar la veracidad de este testimonio, ciertamente Leibniz nunca publicó su hallazgo. Vea *Hist. de l'Ac. de Prusse,* 1750 p. 530.

La siguiente proposición, de la cual un caso especial es nuestro teorema, también será útil para otras investigaciones.

51.

La p-ésima potencia del polinomio $a + b + c +$ etc. es

$$\equiv a^p + b^p + c^p + \text{ etc.}$$

según el módulo p siempre que p sea un número primo.

Demostración. Es evidente que la p-ésima potencia del polinomio $a + b + c +$ etc. está compuesta de términos de la forma $\chi a^\alpha b^\beta c^\gamma$ etc., donde $\alpha + \beta + \gamma +$ etc. $= p$, y χ denota en cuántas maneras p objetos pueden permutarse cuando α, β, γ, etc. de ellas son respectivamente iguales a a, b, c, etc. Pero, antes, en el artículo 41, mostramos que este número siempre es divisible por p, si todos los objetos no son iguales, i.e., si no es que uno de los números α, β, γ, etc. $= p$ y los demás $= 0$. De esto se sigue que todos los términos de $(a + b + c +$ etc.$)^p$, excepto a^p, b^p, c^p, etc., son divisibles por p; por tanto, cuando se trata la congruencia según el módulo p, pueden omitirse todos ellos, y será

$$(a + b + c + \text{ etc.})^p \equiv a^p + b^p + c^p + \text{ etc.} \qquad \text{Q.E.D}$$

Ahora si se ponen todas las cantidades a, b, c, etc. $= 1$ y el número de ellas es $= k$, tendremos $k^p \equiv k$, como en el artículo anterior.

Cuantos números corresponden a un período,
en el cual el número de términos es un divisor dado del número $p - 1$.

52.

Dado que otros números, que no sean divisores del número $p - 1$, no pueden ser los exponentes de las potencias menores congruentes a la unidad, se plantea el problema de si todos los divisores de $p - 1$ disfrutan de esta propiedad, y cuando se clasifican todos estos números no divisibles por p, según el exponente de su potencia menor congruente a la unidad, ¿cuántos de ellos se encuentran para cada uno de los exponentes? Primero conviene observar que basta considerar todos los números positivos de 1 hasta $p - 1$; pues, es evidente que los números congruentes deben

elevarse a una misma potencia para que sean congruentes a la unidad, y por tanto, un número cualquiera debe referirse al mismo exponente al que su residuo menor se refiere. Por consiguiente, tenemos que dedicarnos a hallar cómo, con respecto a esto, se han distribuido los números 1, 2, 3, $\dots p-1$ entre los factores individuales del número $p-1$. Por brevedad, si d es uno de los divisores del número $p-1$ (entre los que también se incluyen 1 y $p-1$) por medio de ψd denotaremos el número de enteros positivos menores que p mismo, cuya d-ésima potencia es la menor congruente a la unidad.

53.

Para que esta investigación pueda entenderse fácilmente, agregamos un ejemplo. Para $p = 19$, los números 1, 2, 3, $\dots 18$ se distribuirán entre los divisores del número 18, de este modo

1	1
2	18
3	7, 11
6	8, 12
9	4, 5, 6, 9, 16, 17
18	2, 3, 10, 13, 14, 15

Por tanto, en este caso, $\psi 1 = 1$, $\psi 2 = 1$, $\psi 3 = 2$, $\psi 6 = 2$, $\psi 9 = 6$, y $\psi 18 = 6$. Un poco de atención enseña que tantos números pertenecen a cualquier exponente como tantos se dan no mayores que él y primos a él, o que en este caso particular, usando la notación del art. 39, $\psi d = \varphi d$. Ahora demostraremos que esta observación es verdadera en general.

I. Si se tiene algún número a *perteneciente* al exponente d (i.e., cuya d-ésima potencia es congruente a la unidad y todas sus potencias inferiores son incongruentes), todas sus potencias a^2, a^3, a^4, $\dots a^d$, o los menores restos de ellas, poseerán también la primera propiedad (la d-ésima potencia de ellas es congruente a la unidad) y puesto que esto puede expresarse diciendo que todos los residuos mínimos de los números a, a^2, a^3, $\dots a^d$ (que son todos diferentes) son raíces de la congruencia $x^d \equiv 1$ y como ésta no puede tener más que d raíces diferentes, es evidente que, excepto los residuos mínimos de los números a, a^2, a^3, $\dots a^d$, no se presenta ningún otro entre los números de 1 a $p-1$ inclusive, cuya d-ésima potencia sea congruente a la unidad. De donde,

es claro que todos los números pertenecientes al exponente d se encuentran entre los residuos mínimos de los números a, a^2, a^3, $\ldots a^d$. Cuáles son y cuántos son ellos, se encontrará como sigue. Si k es un número primo a d, todas las potencias de a^k, cuyos exponentes son $< d$, no serán congruentes a la unidad; pues, sea $\frac{1}{k} \pmod{d} \equiv m$ (ver art. 31), será $a^{km} \equiv a$, por tanto, si la e-ésima potencia de a^k fuera congruente a la unidad y $e < d$, entonces, resultaría $a^{kme} \equiv 1$, y de aquí $a^e \equiv 1$, contrario a la hipótesis. Por eso, es claro que el residuo mínimo de a^k pertenece al exponente d. Si k tiene algún divisor δ común con d, el residuo mínimo de a^k no pertenecerá al exponente d, pues, además la $\frac{d}{\delta}$-ésima potencia es congruente a la unidad (pues, $\frac{kd}{\delta}$ sería divisible por d, o sea $\equiv 0 \pmod{d}$ y por ende $a^{\frac{k\delta}{d}} \equiv 1$). Por consiguiente, se reúnen tantos números pertenecientes al exponente d como números de 1, 2, 3, $\ldots d$ que sean primos a d. Pero, debe recordarse que esta conclusión está basada en la suposición de que ya se tiene un número a perteneciente al exponente d. Por lo cual queda la duda de si es posible que ningún número pertenezca del todo a algún exponente y la conclusión se limita a que ψd sea $= 0$ ó $= \varphi d$.

54.

II. Ahora sean d, d', d'', etc. todos los divisores del número $p-1$: como todos los números 1, 2, 3, $\ldots p-1$ están distribuidos entre éstos,

$$\psi d + \psi d' + \psi d'' + \text{ etc.} = p - 1$$

Pero, en el art. 40, hemos demostrado que

$$\varphi d + \varphi d' + \varphi d'' + \text{ etc.} = p - 1$$

y del artículo anterior, se sigue que ψd es igual o menor que φd, pero no puede ser mayor; de modo semejante para $\psi d'$ y $\varphi d'$, etc., por lo tanto, si algún término (o varios) de ψd, $\psi d'$, $\psi d''$, etc., fuera menor que el término correspondiente de φd, $\varphi d'$, $\varphi d''$, la suma de aquéllos no podría ser igual a la suma de éstos. De esto concluimos que ψd *siempre es igual a* φd, y por eso no depende de la magnitud de $p - 1$.

55.

Un caso particular del artículo anterior merece muchísima atención, a saber, *siempre se presentan números de los cuales ninguna potencia menor que la* $(p-1)$*-ésima es congruente a la unidad,* y hay tantos de ellos entre 1 y $p-1$ como números

menores que $p-1$ y primos a $p-1$. Puesto que la demostración de este teorema no es tan obvia como puede parecer a primera vista, y por la importancia del propio teorema, se puede añadir aquí otra bastante diferente de la anterior; ya que una diversidad de métodos suele ayudar mucho a esclarecer asuntos bastante dudosos. Resuélvase $p-1$ en sus factores primos, de modo que $p-1 = a^\alpha b^\beta c^\gamma$ etc., donde a, b, c, etc. denotan números primos diferentes. Entonces, complementaremos la demostración de este teorema por medio de lo siguiente:

I. Siempre puede encontrarse un número A (o varios) pertenecientes al exponente a^α, e igualmente números B, C, etc., pertenecientes respectivamente a los exponentes b^β, c^γ, etc.

II. El producto de todos los números A, B, C, etc. (o el producto de sus residuos mínimos) pertenece al exponente $p-1$. Esto lo demostramos así:

I. Sea g algún número de 1, 2, 3, $\ldots p-1$ que *no* satisface la congruencia $x^{\frac{p-1}{a}} \equiv 1 \pmod{p}$. Como es de grado $< p-1$, todos estos números no pueden satisfacerla. Entonces, digo que si se pone $= h$ la $\frac{p-1}{a^\alpha}$-ésima potencia de g, este número o su residuo mínimo pertenecerá al exponente a^α.

Pues, es evidente que la potencia a^α-ésima de h será congruente a la $(p-1)$-ésima de g, i.e., a la unidad. Pero, la $a^{\alpha-1}$-ésima potencia de h será congruente a la $\frac{p-1}{a}$-ésima potencia de g, i.e., será no congruente a la unidad, y mucho menos las $a^{\alpha-2}$, $a^{\alpha-3}$, etc. potencias de h pueden ser congruentes a la unidad. Pero, el exponente de la potencia menor de h congruente a la unidad, o el exponente al cual pertenece h debe dividir al número a^α (art. 48). Por lo tanto, puesto que a^α no es divisible por ningún otro número más que por sí mismo y por las potencias menores de a, necesariamente a^α será el exponente al cual pertenece h. *Q. E. D.* Con un método similar se demuestra que existen números que pertenecen a los exponentes b^β, c^γ, etc.

II. Si suponemos que el producto de todos los A, B, C, etc. no pertenece al exponente $p-1$, sino a uno menor t , $p-1$ se dividirá por t (artículo 48), es decir, $\frac{p-1}{t}$ será un entero mayor que la unidad. Sin embargo, con facilidad se ve que este coeficiente o es uno de los números primos a, b, c, etc., o al menos es divisible por uno de ellos (artículo 17), e.g., por a. Con respecto a los otros, la demostración es igual. Así, t dividirá a $\frac{p-1}{a}$; por tanto, el producto ABC etc., elevado a la $\frac{p-1}{a}$-ésima potencia será congruente a la unidad (artículo 46). Pero, es claro que cada uno de los B, C, etc. (excepto A) elevados a la $\frac{p-1}{a}$-ésima potencia serán congruentes a la unidad, cuando los exponentes b^β, c^γ, etc. a los cuales pertenecen dividan a $\frac{p-1}{a}$. Por

eso se tendrá

$$A^{\frac{p-1}{a}} B^{\frac{p-1}{a}} C^{\frac{p-1}{a}} \text{ etc.} \equiv A^{\frac{p-1}{a}} \equiv 1$$

De donde sigue que el exponente, al cual pertenece A, debe dividir a $\frac{p-1}{a}$ (art. 48), i.e., $\frac{p-1}{a^{\alpha+1}}$ es entero; pero $\frac{p-1}{a^{\alpha+1}} = \frac{b^\beta c^\gamma \text{ etc.}}{a}$ no puede ser un número entero (art. 15). Finalmente, hay que concluir que nuestra suposición no puede afirmarse, i.e., el producto ABC etc., en realidad, pertenece al exponente $p-1$. *Q. E. D.*

La segunda demostración parece algo más larga que la primera, pero la primera resulta menos directa que ésta.

56.

Este teorema suministra un ejemplo notable sobre cuánta circunspección se requiere siempre en la teoría de los números, para que no supongamos como cierto lo que no es. El célebre Lambert en su disertación citada arriba, *Acta Erudit.* 1769, p. 127, hace mención a esta proposición, pero no atestigua necesidad alguna de una demostración. Nadie ha intentado una demostración excepto Euler, *Comment. nov. Ac. Petrop. T.* XVIII, 1773, *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia* p. 85 y siguientes. Véase en particular su artículo 37 donde habló bastante sobre la necesidad de una demostración. Pero, la demostración que el docto hombre presentó tiene dos defectos. Uno: en su art. 31, tácitamente supone que la congruencia $x^n \equiv 1$ (traducidos sus argumentos usando nuestra notación) en realidad tiene n raíces diferentes, aunque, sólo había demostrado anteriormente que no puede tener más que n raíces. Otro: dedujo la fórmula de su artículo 34 sólo por inducción.

Raíces primitivas, bases e índices.

57.

Como el ilustre Euler, llamaremos *raíces primitivas* a los números pertenecientes al exponente $p-1$. Por lo tanto, si a es una raíz primitiva, los residuos mínimos de las potencias a, a^2, a^3, $\ldots a^{p-1}$ serán todos diferentes, de donde se deduce fácilmente que entre éstos deben aparecer todos los números 1, 2, 3, $\ldots p-1$, ya que el número de éstos es igual al número de residuos mínimos, i.e., cualquier número no divisible por p es congruente a alguna potencia de a. Esta propiedad notable es de gran utilidad y puede simplificar bastante las operaciones aritméticas respecto a las

congruencias, casi de igual modo como la introducción de los logaritmos simplifica las operaciones de la aritmética común. Elegiremos libremente alguna raíz primitiva como *base,* a la cual referiremos todos los números no divisibles por p, y si $a^e \equiv b \pmod{p}$, llamaremos a e el *índice* de b. Por ejemplo, si para el módulo 19 se toma la raíz primitiva 2 como base, corresponderán

números	1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18.
índices	0. 1. 13. 2. 16. 14. 6. 3. 8. 17. 12. 15. 5. 7. 11. 4. 10. 9.

Es claro, además, al mantener la base constante, que a cada número corresponden varios índices, pero todos ellos serán congruentes según el módulo $p-1$. Por lo que, cuando hay una discusión sobre los índices, aquéllos que son congruentes según el módulo $p-1$ se considerarán equivalentes de la misma manera como los números se consideran equivalentes cuando son congruentes según el módulo p.

Algoritmos de los índices.

58.

Los teoremas que tratan sobre los índices son completamente análogos a los que se refieren a los logaritmos.

El índice del producto compuesto de cualquier número de factores es congruente, según el módulo $p-1$, a la suma de los índices de los factores individuales.

El índice de la potencia de un número cualquiera es congruente, según el módulo $p-1$, al producto del índice del número dado por el exponente de la potencia.

Hemos omitido las demostraciones por su facilidad.

De esto se percibe que si deseamos construir una tabla de la cual se puedan sacar los índices de todos los números según módulos diferentes, de ésta se pueden omitir tanto todos los números mayores al módulo como todos los compuestos. Se ha agregado un ejemplo de este tipo de tabla al final de esta obra, *Tab. I,* donde en la primera columna vertical se colocan los números primos y las potencias de números primos de 3 hasta 97, los cuales se deben considerar como módulos. A la par de éstos están los números tomados como base. Luego siguen los índices de los números primos sucesivos que siempre están arreglados en pequeños bloques de cinco. Arriba los números primos están dispuestos en el mismo orden; de modo que un índice que corresponda a un número primo dado, según un módulo dado, pueda encontrarse fácilmente.

Así por ejemplo si $p = 67$; el índice del número 60, tomado 12 como base, será

$$\equiv 2\,\text{Ind.}\,2 + \text{Ind.}\,3 + \text{Ind.}\,5 \pmod{66} \equiv 58 + 9 + 39 \equiv 40.$$

59.

El índice de un valor cualquiera de la expresión $\frac{a}{b} \pmod{p}$, *(art. 31) es congruente, según el módulo* $p-1$, *a la diferencia de los índices del numerador* a *y del denominador* b, *si es que* a *y* b *no son divisibles por* p.

Sea c, pues, un valor cualquiera; tenemos $bc \equiv a \pmod{p}$ y por lo tanto

$$\text{Ind.}\,b + \text{Ind.}\,c \equiv \text{Ind.}\,a \pmod{p-1}$$

y así

$$\text{Ind.}\,c \equiv \text{Ind.}\,a - \text{Ind.}\,b$$

Entonces, si se tiene una tabla con el índice que corresponde a cualquier número, según cualquier módulo primo, y otra de la cual pueda derivarse el número que corresponda a un índice dado, todas las congruencias de primer grado podrán resolverse muy fácilmente; puesto que todas pueden reducirse a aquéllas cuyo módulo es un primo (art. 30). E.g., la congruenca propuesta

$$29x + 7 \equiv 0 \pmod{47} \qquad \text{será} \qquad x \equiv \frac{-7}{29} \pmod{47}$$

De donde $\text{Ind.}\,x \equiv \text{Ind.}\,-7 - \text{Ind.}\,29 \equiv \text{Ind.}\,40 - \text{Ind.}\,29 \equiv 15 - 43 \equiv 18 \pmod{46}$

Pero, se encuentra el número 3 cuyo índice es 18. Así, $x \equiv 3 \pmod{47}$. No hemos adjuntado la segunda tabla; pero, a cambio de esto, podrá servir otra en su lugar, como mostraremos en la Sección VI.

Sobre las raíces de la congruencia $x^n \equiv A$.

60.

De una manera semejante a como hemos designado en el art. 31 las raíces de las congruencias del primer grado, así, en lo siguiente, presentaremos las raíces de las congruencias puras de grados mayores con un símbolo. Como $\sqrt[n]{A}$ no puede significar más que una raíz de la ecuación $x^n = A$, así al adjuntarse el módulo con el símbolo $\sqrt[n]{A} \pmod{p}$ se denotará cualquier raíz B de la congruencia $x^n \equiv A \pmod{p}$. Decimos que esta expresión $\sqrt[n]{A} \pmod{p}$ tiene tantos valores como

raíces incongruentes mód. p, puesto que todos los que son congruentes según el módulo p se consideran como equivalentes (art. 26). Además, es claro que si A y B son congruentes, según el módulo p las expresiones $\sqrt[n]{A}$ y $\sqrt[n]{B}$ (mod. p) serán equivalentes.

Ahora, si se pone $\sqrt[n]{A} \equiv x \pmod{p}$, será $n \operatorname{Ind}. x \equiv \operatorname{Ind}. A \pmod{p-1}$. De esta congruencia, se deducen, según las reglas de la sección anterior, los valores de $\operatorname{Ind}. x$, y de éstos, los valores correspondientes de x. Fácilmente, se percibe que x tiene tantos valores como raíces de la congruencia $n \operatorname{Ind}. x \equiv \operatorname{Ind}. A \pmod{p-1}$. Es claro, pues, que $\sqrt[n]{A}$ tendrá un único valor, cuando n es primo a $p-1$; sin embargo, cuando los números n y $p-1$ tienen un máximo común divisor δ, $\operatorname{Ind}. x$ tendrá δ valores incongruentes según el módulo $p-1$, y $\sqrt[n]{A}$ tantos valores incongrentes, según p, siempre que $\operatorname{Ind}. A$ sea divisible por δ. Al faltar esta condición, $\sqrt[n]{A}$ no tendrá ningún valor real.

Ejemplo. Búsquense los valores de la expresión $\sqrt[15]{11}$ (mod. 19). Así, debe resolverse la congruencia $15 \operatorname{Ind}. x \equiv \operatorname{Ind}. 11 \equiv 6 \pmod{18}$ y se encontrarán tres valores de $\operatorname{Ind}. x \equiv 4,\ 10,\ 16 \pmod{18}$. Los valores correspondientes de x son 6, 9 y 4.

61.

Por más fácil que este método sea, cuando están adjuntadas las tablas necesarias, no debemos olvidarnos de que éste es indirecto. Por lo tanto, vale la pena investigar cuán poderosos son los métodos directos; trataremos aquí lo que pueda resultar de lo anterior; otros que requieren consideraciones más profundas están reservados para la sección VIII. Iniciamos con el caso más sencillo, donde $A = 1$, es decir, donde se buscan las raíces de la congruencia $x^n \equiv 1 \pmod{p}$. Aquí, por tanto, tomando cualquier raíz primitiva como base, debe resultar $n \operatorname{Ind}. x \equiv 0 \pmod{p-1}$. Esta congruencia, cuando n es primo a $p-1$, tendrá una sola raíz; es decir, $\operatorname{Ind}. x \equiv 0 \pmod{p-1}$. *En este caso* $\sqrt[n]{1} \pmod{p}$ tendrá un único valor, o sea $\equiv 1$. Sin embargo, cuando los números n y $p-1$ tengan máximo común divisor δ, la solución completa de la congruencia $n \operatorname{Ind}. x \equiv 0 \pmod{p-1}$ será $\operatorname{Ind}. x \equiv 0 \pmod{\frac{p-1}{\delta}}$ (ver art. 29): i.e., $\operatorname{Ind}. x$, según el módulo $p-1$, deberá ser congruente a alguno de estos números

$$0, \quad \frac{p-1}{\delta}, \quad \frac{2(p-1)}{\delta}, \quad \frac{3(p-1)}{\delta}, \quad \ldots \frac{(\delta-1)(p-1)}{\delta}$$

o tendrá δ valores incongruentes según el módulo $p-1$, por tanto, también en este caso, x tendrá δ valores diferentes (incongruentes según el módulo p). De donde se percibe que la expresión $\sqrt[\delta]{1}$ también tiene δ valores diferentes, cuyos índices coinciden completamente con los anteriores. Por eso, la expresión $\sqrt[\delta]{1} \pmod p$ equivale totalmente a $\sqrt[n]{1} \pmod p$; i.e., la congruencia $x^\delta \equiv 1 \pmod p$ tiene las mismas raíces que ésta, $x^n \equiv 1 \pmod p$. La anterior, sin embargo, será de grado inferior, si δ y n no son iguales.

Ejemplo. $\sqrt[15]{1} \pmod{19}$ tiene tres valores, pues 3 es el máximo divisor común de los números 15 y 18 y, a la vez, éstos serán valores de la expresión $\sqrt[3]{1}$ (mod. 19). Estos son 1, 7 y 11.

62.

Por medio de esta reducción, no logramos resolver ninguna otra congruencia sino las de la forma $x^n \equiv 1$, donde n es un divisor del número $p-1$. Más adelante, mostraremos que las congruencias de esta forma siempre pueden reducirse, pero lo anterior no basta. Podemos aquí tratar un solo caso, o sea, donde $n = 2$. Es claro que los valores de la expresión $\sqrt[2]{1}$ serán $+1$ y -1, pues, no puede tener más que dos y $+1$ y -1 siempre son incongruentes a menos que el módulo sea $= 2$, en cuyo caso $\sqrt[2]{1}$ puede tener un solo valor, como se puede ver. De donde, por consiguiente, sigue que $+1$ y -1 serán también los valores de la expresión $\sqrt[2m]{1}$ cuando m es primo a $\frac{p-1}{2}$. Esto siempre sucede cuando el módulo es de esta clase, con tal que sea un número absolutamente primo (a menos que $p-1 = 2m$, en tal caso todos los números 1, 2, 3, $\ldots p-1$ son raíces), e.g., cuando $p = 3, 5, 7, 11, 23, 47, 59, 83, 107$ etc. Se adjuntará aquí como corolario que el índice de -1 siempre es $\equiv \frac{p-1}{2} \pmod{p-1}$ cualquiera que sea la raíz primitiva tomada como base. Pues, $2\,\mathrm{Ind.}\,(-1) \equiv 0 \pmod{p-1}$. Así, $\mathrm{Ind.}\,(-1)$ será $\equiv 0$, ó $\equiv \frac{p-1}{2} \pmod{p-1}$. Pero, 0 siempre es el índice de $+1$, y $+1$ y -1 siempre deben tener diferentes índices (excepto el caso $p = 2$, al que no vale la pena referirse aquí).

63.

Hemos mostrado, en el art. 60, que la expresión $\sqrt[n]{A} \pmod p$ tiene δ valores diferentes, o no tiene ninguno, si δ es el máximo común divisor de los números n y $p-1$. Ahora, del mismo modo como mostramos que $\sqrt[n]{A}$ y $\sqrt[\delta]{A}$ son equivalentes si $A \equiv 1$, demostramos más generalmente que la expresión $\sqrt[n]{A}$ siempre puede reducirse

a la otra $\sqrt[\delta]{B}$, a la cual equivalga. Pues, denotado un valor cualquiera de éstos por x, será $x^n \equiv A$; ahora, sea t un valor cualquiera de la expresión $\frac{\delta}{n} \pmod{p-1}$, la cual tiene valores reales como se percibe en el art. 31, será $x^{tn} \equiv A^t$, pero $x^{tn} \equiv x^\delta$, puesto que $tn \equiv \delta \pmod{p-1}$. Por tanto, $x^\delta \equiv A^t$ y cualquier valor de $\sqrt[n]{A}$ será también un valor de $\sqrt[\delta]{A^t}$. Por lo tanto, cuando $\sqrt[n]{A}$ tiene valores reales, será totalmente equivalente a la expresión $\sqrt[\delta]{A^t}$, puesto que aquélla ni tiene otros valores diferentes a la anterior, ni tiene menos. Es posible que $\sqrt[n]{A}$ no tenga ningún valor real aún cuando $\sqrt[\delta]{A^t}$ tenga valores reales.

Ejemplo. Si se buscan los valores de la expresión $\sqrt[21]{2} \pmod{31}$, el máximo común divisor de los números 21 y 30 será 3, y éste es un valor de la expresión $\frac{3}{21} \pmod{30}$; por tanto, si $\sqrt[21]{2}$ tiene valores reales, equivaldrá a la expresión $\sqrt[3]{2^3}$ o sea $\sqrt[3]{8}$, se encontrará en verdad que los valores de la expresión posterior, que son 2, 10, 19, también satisfacen la anterior.

64.

Para no intentar realizar en vano esta operación, conviene investigar una regla por medio de la cual pueda deducirse de inmediato si $\sqrt[n]{A}$ admite valores reales o no. Si se tiene una tabla de índices, el asunto es claro, pues, es claro, en el art. 60, que se tendrán valores reales si el índice de A, tomando cualquier raíz primitiva como base, es divisible por δ; pero si no lo es, no se tendrán. No obstante, esto puede hallarse sin esa tabla. Pues, al poner el índice de $A = k$, si es divisible por δ, será $\frac{k(p-1)}{\delta}$ divisible por $p-1$ y vice-versa. Pero, el índice del número $A^{\frac{p-1}{\delta}}$ será $\frac{k(p-1)}{\delta}$. Por lo cual, si $\sqrt[n]{A} \pmod{p}$ tiene valores reales, $A^{\frac{p-1}{\delta}}$ será congruente a la unidad; en caso contrario, será incongruente. Así, en el ejemplo del artículo anterior, se tiene $2^{10} = 1024 \equiv 1 \pmod{31}$, de donde se concluye que $\sqrt[21]{2} \pmod{31}$ tiene valores reales. De modo semejante, resulta cierto que $\sqrt[2]{-1} \pmod{p}$ siempre tiene dos valores reales cuando p es de la forma $4m+1$, pero ninguno cuando p es de la forma $4m+3$, puesto que $(-1)^{2m} = 1$ y $(-1)^{2m+1} = -1$. Este elegante teorema se enuncia ordinariamente así: *si p es número primo de la forma $4m+1$, se puede encontrar un cuadrado a^2, de modo que a^2+1 sea divisible por p, pero si al contrario, p es de la forma $4m-1$, no se puede encontrar tal cuadrado.* De esta forma fue demostrado por el ilustre Euler, en *Comm. nov. Acad. Petrop.* XVIII, p. 112 del año 1773. El ya había presentado otra demostración mucho antes en 1760, *Comm. nov.* V, p. 5. En una disertación anterior, *Comm. nov.* IV, p. 25, todavía no la había perfeccionado. Luego, el ilustre Lagrange

presentó una demostración del teorema, *Nouveaux Mém. de l'Ac. de Berlín,* 1775, p. 342. Presentaremos otra demostración, en la siguiente sección, específicamente dedicada a este argumento.

65.

Después de que hemos hablado de reducir todas las expresiones $\sqrt[n]{A} \pmod{p}$ a otras, donde n es divisor del número $p-1$, y hemos encontrado un criterio de si admite o no valores reales, consideraremos más precisamente tales expresiones $\sqrt[n]{A} \pmod{p}$, donde n es divisor de $p-1$. Primero mostraremos qué relación tienen los valores individuales de la expresión entre sí; luego indicaremos unos artificios, con cuya ayuda muchas veces puede encontrarse un valor de la expresión.

Primero. Cuando $A \equiv 1$ y r es alguno de los n valores de la expresión $\sqrt[n]{1} \pmod{p}$, ó $r^n \equiv 1 \pmod{p}$, también todas las potencias de este r serán valores de esta expresión; pero de ellos, tantos serán diferentes como unidades tenga el exponente al cual r pertenece (art. 48). Si, por lo tanto, r es el valor que pertenece al exponente n, estas potencias r, r^2, r^3, $\ldots r^n$ de este mismo r (donde en el lugar de la última puede sustituirse la unidad) involucrarán todos los valores de la expresión $\sqrt[n]{1} \pmod{p}$. En la sección VIII explicaremos bastante cuáles métodos existen para encontrar aquellos valores que pertenecen al exponente n.

Segundo. Cuando A es incongruente a la unidad, y conocemos un valor de la expresión $\sqrt[n]{A} \pmod{p}$, digamos z, los restantes pueden deducirse del siguiente modo. Sean los valores de la expresión $\sqrt[n]{1}$

$$1,\ r,\ r^2,\ \ldots r^{n-1}$$

(como mostramos arriba). Entonces todos los valores de la expresión $\sqrt[n]{A}$ serán

$$z,\ zr,\ zr^2,\ \ldots zr^{n-1}.$$

Está claro, pues, que todos éstos satisfacen la congruencia $x^n \equiv A$: pongamos cualquiera de ellos $\equiv zr^k$, la n-esima potencia de ella, $z^n r^{nk}$, por ser $r^n \equiv 1$ y $z^n \equiv A$, será congruente a A. Todos son diferentes como se deduce fácilmente del art. 23; pero la expresión $\sqrt[n]{A}$ no puede tener más que estos n valores. Así, por ejemplo, si un valor de una expresión $\sqrt[2]{A}$ es z, el otro será $-z$. Finalmente, de esto se debe concluir que no se pueden encontrar todos los valores de la expresión $\sqrt[n]{A}$ si no se conocen igualmente todos los valores de la expresión $\sqrt[n]{1}$.

66.

Lo segundo que nos habíamos propuesto mostrar era en cuál caso un valor de la expresión $\sqrt[n]{A} \pmod{p}$ puede encontrarse directamente (donde se supone que n es un divisor de $p-1$). Esto resulta cuando algún valor es congruente a alguna potencia de A, lo cual no es tan raro, y no será superfluo detenernos en ello. Sea tal valor z, *si existe*, o sea $z \equiv A^k$ y $A \equiv z^n \pmod{p}$. De esto se deduce que $A \equiv A^{kn}$; por lo tanto, si se tiene un número k, de modo que $A \equiv A^{kn}$, A^k será el valor buscado. Pero esto equivaldrá aquí a la condición siguiente, $1 \equiv kn \pmod{t}$, denotando a t el exponente al cual pertenece A (art. 46, 48). Para que esta congruencia sea posible, se requiere que n sea primo a t. En este caso será $k \equiv \frac{1}{n} \pmod{t}$, pero si t y n tienen un divisor común, ningún valor z puede ser congruente a alguna potencia de A.

67.

No obstante, como conviene conocer a t para esta solución, veamos cómo podemos proceder si desconocemos este número. Primero, se percibe fácilmente que t debe dividir a $\frac{p-1}{n}$, si es que $\sqrt[n]{A} \pmod{p}$ tiene valores reales, como siempre lo hemos supuesto aquí. Sea pues y una solución cualquiera, entonces tendremos $y^{p-1} \equiv 1$ y $y^n \equiv A \pmod{p}$; por lo cual elevando las partes de la última congruencia a la $\frac{p-1}{n}$-ésima potencia resultará $A^{\frac{p-1}{n}} \equiv 1$; de tal modo $\frac{p-1}{n}$ es divisible por t (art. 48). Ahora, si $\frac{p-1}{n}$ es primo a n, la congruencia del artículo anterior, $kn \equiv 1$, no sólo podrá resolverse según el módulo $\frac{p-1}{n}$, sino claramente el valor de k que satisface a esta congruencia según este módulo también la satisfará según el módulo t, el cual divide a $\frac{p-1}{n}$ (art. 5). Por tanto, se ha encontrado lo buscado. Sin embargo, si $\frac{p-1}{n}$ no es primo a n, se eliminarán todos los factores primos de $\frac{p-1}{n}$, que a la vez dividen a n. Por eso, encontraremos un número $\frac{p-1}{nq}$, primo a n, donde q denota el producto de todos los factores primos que hemos eliminado. Ahora, si la condición que logramos en el artículo anterior, que t sea primo a n, tiene lugar, t no sólo será primo a q sino también dividirá a $\frac{p-1}{nq}$. Por eso, si se resuelve la congruencia $kn \equiv 1 \pmod{\frac{p-1}{nq}}$ (lo que puede ser, puesto que n es primo a $\frac{p-1}{nq}$), el valor k también satisfará la congruencia, según el módulo t; lo cual se buscaba. Todo este artificio consiste en hallar un número que pueda funcionar en vez de t, el cual no conocemos. Aunque siempre conviene recordar: hemos supuesto que, cuando $\frac{p-1}{n}$ no es primo a n, cabe la condición del artículo anterior, pero si no es cierta, todas las conclusiones serían erróneas. Sin embargo, si aún siguiendo las reglas dadas, se encuentra un valor

para z, cuya n-ésima potencia es incongruente a A, esto sería una muestra de que la condición no puede satisfacerse y que el método no puede emplearse del todo.

68.

Pero, en este caso también puede ser ventajoso haber realizado este trabajo y vale la pena investigar cómo este valor falso se relaciona con los verdaderos. Así, supongamos que los números k y z están bien determinados, pero que z^n no es $\equiv A \pmod{p}$. Entonces, si sólo pueden determinarse valores de la expresión $\sqrt[n]{\frac{A}{z^n}} \pmod{p}$, multiplicando cada uno de estos valores por z, obtendremos los valores de $\sqrt[n]{A}$. Pues si v es algún valor de $\sqrt[n]{\frac{A}{z^n}}$: será $(vz)^n \equiv A$. Pero la expresión $\sqrt[n]{\frac{A}{z^n}}$ es más simple que $\sqrt[n]{A}$, puesto que $\frac{A}{z^n} \pmod{p}$ con frecuencia pertenece a un exponente menor que A. Es decir, si d es el máximo común divisor de los números t y q, $\frac{A}{z^n} \pmod{p}$ pertenecerá al exponente d, como se demostrará ahora. Sustituyendo por el valor z, será $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}} \pmod{p}$. Pero, $kn-1$ es divisible por $\frac{p-1}{nq}$ (artículo anterior), $\frac{p-1}{n}$ por t (ibid.) o sea $\frac{p-1}{nd}$ por $\frac{t}{d}$. Ahora bien $\frac{t}{d}$ es primo a $\frac{q}{d}$ (hip.), así $\frac{p-1}{nd}$ será divisible por $\frac{tq}{d^2}$ o bien $\frac{p-1}{nq}$ por $\frac{t}{d}$. También $kn-1$ será divisible por $\frac{t}{d}$ y $(kn-1)d$ por t. Por lo tanto, $A^{(kn-1)d} \equiv 1 \pmod{p}$. De donde se deduce fácilmente que $\frac{A}{z^n}$, elevada a la d-ésima potencia, será congruente a la unidad. El que $\frac{A}{z^n}$ no pueda pertenecer a un exponente menor que d, puede demostrarse fácilmente; pero, ya que no se requiere para nuestros fines, no nos detendremos en esto. Podemos estar seguros que $\frac{A}{z^n} \pmod{p}$ siempre pertenecerá a un exponente menor que A, excepto en un caso único, cuando t divide a q; de donde $d = t$.

Pero, ¿de qué sirve que $\frac{A}{z^n}$ pertenezca a un exponente menor que A? Se presenta mayor cantidad de números que pueden ser A que los que pueden ser $\frac{A}{z^n}$, y cuando haya ocasión de desarrollar varias expresiones $\sqrt[n]{A}$ según un mismo módulo, tendremos la ventaja de derivar varios resultados de una misma fuente. Así, por ejemplo, siempre será posible determinar al menos un valor de la expresión $\sqrt[2]{A}$ (mod. 29), si sólo se conocen los valores de la expresión $\sqrt[2]{-1}$ (que son ± 12). Del artículo anterior se conoce fácilmente que un valor de esta expresión siempre puede determinarse directamente, ya sea cuando t es impar y $d = 2$ o cuando t es par. Excepto para -1, ningún otro número pertenece al exponente 2.

Ejemplos. Búsquese $\sqrt[3]{31} \pmod{37}$. Aquí, $p-1 = 36$, $n = 3$, $\frac{p-1}{3} = 12$, y así $q = 3$. Por lo tanto, debe ser $3k \equiv 1 \pmod{4}$, lo cual se obtiene poniendo $k = 3$. Aquí $z \equiv 31^3 \pmod{37} \equiv 6$, se halla realmente $6^3 \equiv 31 \pmod{37}$. Si los

valores de la expresión $\sqrt[3]{1} \pmod{37}$ son conocidos, también los restantes valores de la expresión $\sqrt[3]{6}$ pueden determinarse. Los valores de $\sqrt[3]{1} \pmod{37}$ son 1, 10 y 26. Al multiplicarlos por 6, se producen los restantes $\equiv 23$ y 8.

Sin embargo, si se busca el valor de la expresión $\sqrt[2]{3} \pmod{37}$, será $n = 2$, $\frac{p-1}{n} = 18$, y de aquí $q = 2$. Por tanto, debe ser $2k \equiv 1 \pmod{9}$, de donde resulta $k \equiv 5 \pmod{9}$. Por consiguiente, $z \equiv 3^5 \equiv 21 \pmod{37}$; pero 21^2 no es $\equiv 3$, sino $\equiv 34$. Así, $\frac{3}{34} \pmod{37} \equiv -1$, y $\sqrt[2]{-1} \pmod{37} \equiv \pm 6$; de donde se obtendrán los valores verdaderos $\pm 6 \cdot 21 \equiv \pm 15$.

Esto es casi todo lo que se puede decir acerca del desarrollo de tales expresiones. Es evidente que los métodos directos con frecuencia resultan bastante largos; pero esto es cierto para casi todos los métodos directos en la teoría de los números; por esto, consideramos que debemos demostrarlo. También, conviene observar que no es de nuestro interés explicar los artificios particulares que se presentan aquí.

La conexión entre los indices en sistemas diferentes.

69.

Volvemos ahora a las raíces que llamamos primitivas. Hemos mostrado, al tomar una raíz primitiva cualquiera como base, que todos los números, cuyos índices son primos a $p-1$, también serán raíces primitivas, y ninguno aparte de éstos. A la vez se conoce el número de raíces primitivas. Véase art. 53. En general, queda a nuestro arbitrio saber cuál raíz primitiva escogeremos como base. De esto se percibe, también aquí, como en el cálculo logarítmico, que pueden presentarse diferentes sistemas*). Veamos las relaciones que los conectan. Sean a y b dos raíces primitivas, sea m otro número. Cuando se toma a a como base, el índice del número $b \equiv \beta$, pero el índice del número $m \equiv \mu \pmod{p-1}$; cuando se toma b como base, el índice del número $a \equiv \alpha$, el índice de b sin embargo $\equiv \nu \pmod{p-1}$. Entonces será $\alpha\beta \equiv 1 \pmod{p-1}$; puesto que $a^\beta \equiv b$, de donde $a^{\alpha\beta} \equiv b^\alpha \equiv a \pmod{p}$ (por hipótesis), por lo tanto $\alpha\beta \equiv 1 \pmod{p-1}$. Mediante un razonamiento similar, se descubre que $\nu \equiv \alpha\mu$, por eso $\mu \equiv \beta\nu \pmod{p-1}$. Por lo tanto, si se ha construido una tabla de índices para la base a, fácilmente puede convertirse en otra, donde la base es b. Pues si para la base a el índice de b es $\equiv \beta$, para la base b el índice de a será

*) Difieren en esto: en los logaritmos el número de sistemas es infinito; aquí hay tantos como el número de raíces primitivas. Obviamente, bases congruentes producen los mismos sistemas.

$\equiv \frac{1}{\beta} \pmod{p-1}$, y multiplicando todos los índices de la tabla por este número, se tendrán todos los índices para la base b.

70.

Aunque un número dado puede tener varios índices, tomadas unas u otras raíces primitivas como base, todas concuerdan en esto: todos tendrán el mismo máximo común divisor con $p-1$. Pues, si por la base a, el índice del número dado es m, pero por la base b es n, y si los máximos comunes divisores μ y ν con $p-1$ se suponen diferentes, uno de ellos será mayor, por ejemplo $\mu > \nu$, y por eso n no dividirá a μ. Pero, denotado el índice de a por α, cuando se toma a b como base, será (artículo anterior) $n \equiv \alpha m \pmod{p-1}$, de donde μ dividirá a n. *Q. E. A.*

Se percibe también que este máximo común divisor de los índices de un número dado y de $p-1$ no depende de la base porque es igual a $\frac{p-1}{t}$, donde t denota el exponente al cual pertenece el número sobre cuyos índices se trata. Pues si el índice para una base cualquiera es k, t será el número menor que, multiplicado por k, resultará un múltiplo de $p-1$ (excepto cero) (véanse artículos 48 y 58), o sea, el valor menor de la expresión $\frac{0}{k} \pmod{p-1}$ excepto cero. No obstante, que esto es igual al máximo común divisor de los números k y $p-1$, se obtiene del artículo 29 sin dificultad.

71.

Además se demuestra fácilmente que la base siempre puede tomarse de modo que un número que pertenece al exponente t tiene cualquier índice dado cuyo máximo común divisor con $p-1$ es $= \frac{p-1}{t}$. Por brevedad, designaremos éste por d, si el índice propuesto es $\equiv dm$, y el índice del número propuesto $\equiv dn$, cuando se toma cualquier raíz primitiva como base, entonces m y n serán primos a $\frac{p-1}{d}$, o sea a t. Entonces, si ε es el valor de la expresión $\frac{dn}{dm} \pmod{p-1}$ y a la vez es primo a $p-1$, a^{ε} será una raíz primitiva. Tomada ésta como base, el número propuesto producirá el índice dm (pues será $a^{\varepsilon dm} \equiv a^{dn} \equiv$ número propuesto). Pero, del modo siguiente se demuestra que la expresión $\frac{dn}{dm} \pmod{p-1}$ admite valores primos a $p-1$. Esta expresión equivaldrá a: $\frac{n}{m} \pmod{\frac{p-1}{d}}$ o sea $\frac{n}{m} \pmod{t}$ (véase art. 31, 2). Todos sus valores serán primos a t; ya que, si algún valor e tuviera un divisor común con t, este divisor también debería dividir a me, por tanto, también me es congruente a n según t, contrariamente a la hipótesis de que n es primo a t. Por lo tanto, cuando todos los

divisores primos de $p-1$ también dividen a t, todos los valores de la expresión $\frac{n}{m}$ (mod. t) serán primos a $p-1$, y el número de ellos $= d$. Sin embargo, cuando $p-1$ involucra otros divisores primos f, g, h, etc., que no dividen a t, se toma cualquier valor de la expresión $\frac{n}{m}$ (mod. t) $\equiv e$. Entonces, puesto que t, f, g, h, etc., son primos entre sí, puede hallarse un número ε que es congruente a e según el módulo t, pero según f, g, h, etc. es congruente a números cualesquiera primos a éstos respectivamente (art. 32). Por eso tal número no será divisible por ningún factor primo de $p-1$, por lo tanto será primo a $p-1$, tal como se esperaba. Finalmente, sin dificultad alguna, se deduce de la teoría de las combinaciones que el número de tales valores será $= \frac{p-1}{t} \cdot \frac{f-1}{f} \cdot \frac{g-1}{g} \cdot \frac{h-1}{h} \cdot$ etc.; pero para que no se extienda mucho esta disgresión, hemos omitido la demostración, puesto que no nos concierne.

Bases adaptadas para usos especiales.

72.

Aunque generalmente sea muy arbitrario cuál raíz primitiva se tomará como base, a veces ciertas bases pueden presentar algunas conveniencias especiales. En la tabla I, siempre hemos tomado el número 10 como la base cuando éste era raíz primitiva; de otra manera hemos determinado la base de modo que el índice del número 10 sea el menor posible, i.e., $= \frac{p-1}{t}$, donde t denota el exponente al cual perteneció 10. Pero, lo que ganamos con esto, lo presentaremos en la Sección VI, donde la misma tabla se aplicará para otros fines. Sin embargo, puesto que aquí esto todavía puede permanecer un poco arbitrario, como aparece en el artículo anterior: para establecer algo fijo, de todas las raíces primitivas, eligimos siempre como base la *menor*. Así, para $p = 73$, donde $t = 8$ y $d = 9$, a^{ε} tiene $\frac{72 \cdot 2}{8 \cdot 3}$, i.e., 6 valores que son 5, 14, 20, 28, 39, 40. Por esto, tomamos el mínimo, 5, como base.

Método para la determinación de las raíces primitivas.

73.

Los métodos para encontrar las raíces primitivas se basan en su mayoría en el tanteo. Si se reune lo que hemos aprendido en el artículo 55, con lo que diremos adelante sobre las soluciones de la congruencia $x^n \equiv 1$, se tendrá casi todo lo que puede lograrse con los métodos directos. El ilustre Euler reconoce (*Opuscula Analytica, T.* I, *p.* 152) que parece extremadamente difícil encontrar estos números, y se refiere a su naturaleza como uno de los misterios más grandes de los números. Pero,

pueden determinarse bastante rápidamente al intentarlo de la siguiente manera. Un conocedor sabrá evitar operaciones prolijas por medio de varios artificios particulares: pero esto se aprende mas rápidamente con práctica que con preceptos.

1^o. Tómese libremente un número a, primo a p (siempre designamos el módulo con esta letra) (casi siempre lleva a los cálculos cortos si escogemos el menor posible, e.g., el número 2); luego determínese su período (art. 46), i.e., los residuos mínimos de sus potencias, hasta encontrar la potencia a^t cuyo residuo mínimo sea 1*). Ahora, si $t = p - 1$, a es una raíz primitiva.

2^o. Pero, si $t < p-1$, se toma otro número b que no está en el período de a, y de modo semejante se investigará su período. Al designar por u el exponente al cual pertenece b, se percibe fácilmente que u ni puede ser igual a t, ni a un factor de t; de hecho en los dos casos sería $b^t \equiv 1$; lo cual no puede ser, puesto que el período de a contiene todos los números cuya t-ésima potencia es congruente a la unidad (art. 53). Ahora si u es $= p - 1$, b será una raíz primitiva; pero si u no es $= p - 1$, sino un múltiplo de t, hemos logrado esto: que conocemos un número perteneciente a un exponente mayor, de modo que nuestro propósito, encontrar el número perteneciente al exponente *máximo,* está próximo. Pero si u no es $= p-1$, ni a un múltiplo de t, no obstante, podemos encontrar un número u que pertenece a un exponente mayor que t, a saber, al exponente igual al mínimo común múltiplo de los números t y u. Sea éste $= y$, así resuélvase y en dos factores primos entre sí, m y n, de modo que uno divide a t, y el otro a u†). Entonces, la $\frac{t}{m}$-ésima potencia de a será $\equiv A$, la $\frac{u}{n}$-ésima potencia de b será $\equiv B \pmod{p}$, y el producto AB será un número perteneciente al exponente y. Es fácil percibir que A pertenece al exponente m, y B al exponente n, de modo que el producto AB pertenecerá a mn, puesto que m y n son primos entre sí. Esto podrá demostrarse prácticamente del mismo modo como en el art. 55, II.

3^o. Ahora, si $y = p-1$, AB será una raíz primitiva. Si no es el caso, entonces de igual manera que antes se deberá tomar otro número que no aparece en el período de AB. Esto, o bien, será una raíz primitiva, o pertenecerá a un exponente mayor que y, o por medio de él (como antes) podrá encontrarse un número que pertenece a un exponente mayor que y. Por tanto, como los números que resultan de repeticiones

*) Se percibe con facilidad que no es necesario conocer estas potencias, puesto que el residuo mínimo puede obtenerse fácilmente de un residuo mínimo de la potencia anterior.

†) Del art. 18 se deriva cómo se puede hacer sin dificultad. Resuélvase y en factores que son o bien números primos diferentes, o bien potencias de números primos diferentes. Cada uno de ellos dividirá a t o a u (o a ambos). Asígnense cada uno o a t o a u según el cual él divida por él: cuando alguno divide a ambos, se le puede asignar arbitrariamente. Sea m el producto de los asignados a t, el de los otros $= n$. Está claro que m divide a t, n divide a u, y $mn = y$.

de esta operación pertenecen a exponentes continuamente crecientes; es claro que, finalmente, se debe encontrar un número que pertenezca al exponente mayor, i.e., una raíz primitiva. *Q. E. F.*

74.

Estas reglas anteriores serán más claras mediante un ejemplo. Sea $p = 73$ para el cual se busca una raíz primitiva. Intentaremos primero con el número 2, cuyo período es el siguiente:

1.2.4.8.16.32.64.55.37.1 etc.
0.1.2.3. 4. 5. 6. 7. 8.9 etc.

Puesto que ya la potencia del exponente 9 es congruente a la unidad, 2 no es una raíz primitiva. Pruébese con otro número que no aparece en el período de 2, por ejemplo 3, cuyo período es éste:

1.3.9.27.8.24.72.70.64.46.65.49. 1 etc.
0.1.2. 3.4. 5. 6. 7. 8. 9.10.11.12 etc.

Por lo tanto, 3 tampoco es una raíz primitiva. En cambio, el mínimo común múltiplo de los exponentes a los cuales pertenecen 2 y 3 (i.e., los números 9 y 12) es 36, el cual se resuelve en los factores 9 y 4 según los preceptos del artículo anterior. Así que al elevarse 2 a la potencia $\frac{9}{9}$, i.e., reteniendo el número 2; y 3 a la potencia 3: el producto de éstos es 54, que por tanto pertenecerá al exponente 36. Si finalmente se calcula el período de 54, y se intenta con un número no contenido en él, por ejemplo, el número 5, se descubrirá que es una raíz primitiva.

Varios teoremas sobre los períodos y las raíces primitivas.

75.

Antes de dejar este argumento, presentaremos algunas proposiciones, a las que por su simplicidad conviene prestarles atención.

El producto de todos los términos del período de un número cualquiera es $\equiv 1$*, cuando el número de ellos o el exponente al cual pertenece el número es impar, y* $\equiv -1$ *cuando este exponente es par.*

Ejemplo. Para el módulo 13 el período del número 5 consta de estos términos 1, 5, 12, 8, cuyo producto $480 \equiv -1 \pmod{13}$.

Según el mismo módulo, el período del número 3 consta de los términos 1, 3, 9, cuyo producto $27 \equiv 1 \pmod{13}$.

Demostración. Sea t el exponente al cual pertenece un número, y $\frac{p-1}{t}$ el índice del número, lo cual siempre puede ser si se determina debidamente la base (art. 71). Entonces, el índice del producto de todos los términos del período será

$$\equiv (1+2+3+ \text{ etc.} + t-1)\frac{p-1}{t} = \frac{(t-1)(p-1)}{2}$$

i.e., $\equiv 0 \pmod{p-1}$ cuando t es impar, y $\equiv \frac{p-1}{2}$ cuando t es par; por tanto, en el primer caso este producto $\equiv 1 \pmod{p}$; en el último $\equiv -1 \pmod{p}$, (art. 62). *Q. E. D.*

76.

Si ese número en el teorema precedente es una raíz primitiva, su período comprenderá todos los números 1, 2, 3, $\ldots p-1$, cuyo producto siempre $\equiv -1$ (pues $p-1$ es siempre par, excepto un caso, $p=2$, en el cual -1 y $+1$ son equivalentes). Este elegante teorema suele enunciarse así: *el producto de todos los números menores que un número primo dado, sumado a uno, es divisible por este primo.* Fue publicado primero por el célebre Waring, y adscrito a Wilson, (*Meditt. algebr.*, tercera edición, *p.* 380). Pero ninguno pudo demostrarlo, y el célebre Waring confesó que la demostración parecía más difícil porque ninguna *notación* puede confeccionarse para expresar un número primo. Pero a nuestro juicio tales verdades debían percibirse por medio de las nociones más que por las notaciones. Después, el ilustre Lagrange presentó una demostración (*Nouv. Mém. de l'Ac. Berlin,* 1771). Se basa en la consideración de los coeficientes originados en el desarrollo del producto

$$(x+1)(x+2)(x+3)\ldots(x+p-1).$$

De hecho, con poner este producto

$$\equiv x^{p-1} + Ax^{p-2} + Bx^{p-3} + \text{ etc.} + Mx + N$$

los coeficientes A, B, etc., M serán divisibles por p, y N será $= 1\cdot 2\cdot 3\cdot \ldots \cdot p-1$. Ahora, para $x=1$, el producto será divisible por p; entonces será $\equiv 1+N \pmod{p}$, de donde necesariamente $1+N$ podrá dividirse por p.

Finalmente, el ilustre Euler ha presentado una demostración en *Opusc. analyt. T.* I. *p.* 329 que concuerda con la expuesta por nosotros. Pero si tan distinguidos matemáticos no han considerado sin mérito a este teorema para sus meditaciones, esperamos no ser censurados si adjuntamos todavía otra demostración.

77.

Cuando según el módulo p, el producto de dos números a y b es congruente a la unidad, llamaremos a los números a y b *asociados,* tal como lo hizo Euler. Entonces, según la sección anterior, cualquier número positivo menor que p tendrá un único asociado positivo menor que p. Puede demostrarse fácilmente que de los números 1, 2, 3,... $p-1$, los únicos asociados de sí mismos son 1 y $p-1$: pues los números asociados de sí mismos serán raíces de la congruencia $x^2 \equiv 1$; que es de segundo grado, por tanto no puede tener más que dos raíces, i.e., ninguna otra más que 1 y $p-1$. Excluidos éstos de los números restantes, 2, 3, $\ldots p-2$ estarán asociados siempre en pares; por tanto el producto de ellos será $\equiv 1$, de donde el producto de todos 1, 2, 3, $\ldots p-1$, será $\equiv p-1$ o sea $\equiv -1$. *Q. E. D.*

Por ejemplo, para $p = 13$, se asocian los números 2, 3, 4, $\ldots 11$ así: 2 con 7; 3 con 9; 4 con 10; 5 con 8; 6 con 11; entonces $2 \cdot 7 \equiv 1$; $3 \cdot 9 \equiv 1$ etc. Por tanto $2 \cdot 3 \cdot 4 \cdot \ldots 11 \equiv 1$, y $1 \cdot 2 \cdot 3 \ldots 12 \equiv -1$.

78.

El teorema de Wilson puede exponerse más generalmente así: *el producto de todos los números, a la vez menores que cualquier número dado A y primos a él mismo, es congruente, según el módulo A, a la unidad tomada positiva o negativamente.* Se debe tomar la unidad negativamente cuando A es de la forma p^m, o bien $2p^m$, donde p denota un número primo diferente de 2, y además cuando $A = 4$; se toma positivamente en todos los casos restantes. El teorema, como fue presentado por el célebre Wilson, está contenido bajo el primer caso. Por ejemplo, para $A = 15$, el producto de los números 1, 2, 4, 7, 8, 11, 13, 14 es $\equiv 1 \pmod{15}$. Por brevedad no adjuntamos la demostración: observamos solamente que puede completarse de modo semejante al del artículo anterior, excepto que la congruencia $x^2 \equiv 1$ puede tener más de dos raíces, las cuales exigen ciertas consideraciones peculiares. También la demostración puede derivarse de la consideración de los índices, similarmente como en el artículo 75, si se agrega lo que pronto expondremos sobre los módulos compuestos.

79.

Volvemos a la enumeración de otras proposiciones (art. 75).

La suma de todos los términos del período de un número cualquiera es $\equiv 0$, como en el ejemplo del artículo 75, $1 + 5 + 12 + 8 = 26 \equiv 0 \pmod{13}$.

Demostración. Sea a el número de cuyo período se trata, y t el exponente al cual pertenece. La suma de todos los términos del período será:

$$\equiv 1 + a + a^2 + a^3 + \text{ etc.} + a^{t-1} \equiv \frac{a^t - 1}{a - 1} \pmod{p}$$

Pero, $a^t - 1 \equiv 0$: por tanto esta suma siempre será $\equiv 0$ (art. 22), a menos que por casualidad $a-1$ sea divisible por p, o sea $a \equiv 1$; por lo tanto, este caso debe excluirse si deseamos llamar *período* a un solo término.

80.

El producto de todas las raíces primitivas es $\equiv 1$, excepto el caso único $p = 3$; pues en este se presenta una sola raíz primitiva, 2.

Demostración. Si se toma una raíz primitiva cualquiera como base, los índices de todas las raíces primitivas serán números primos a $p-1$ y a la vez menores que él. Pero la suma de estos números, i.e., el índice del producto de todas las raíces primitivas, es $\equiv 0 \pmod{p-1}$, de donde el producto $\equiv 1 \pmod{p}$. En efecto se percibe fácilmente que si k es un número primo a $p-1$, también $p-1-k$ será primo a $p-1$, y por lo tanto la suma de los números primos a $p-1$ se compone de pares cuya suma es divisible por $p-1$ (aunque k nunca puede ser igual a $p-1-k$ excepto en el caso $p-1=2$, o sea $p=3$, el cual excluimos; pues es claro, en todos los casos restantes que $\frac{p-1}{2}$ no es primo a $p-1$).

81.

La suma de todas las raíces primitivas es o bien $\equiv 0$ (cuando $p-1$ es divisible por algún *cuadrado*), *o bien* $\equiv \pm 1 \pmod{p}$ (cuando $p-1$ es un producto de números primos diferentes; si el número de ellos es par, se toma el signo positivo, pero si es impar, se toma el negativo.)

Ejemplo. 1^o. Para $p = 13$, se tienen las raíces primitivas 2, 6, 7, 11, cuya suma $26 \equiv 0 \pmod{13}$.

2^o. Para $p = 11$, las raíces primitivas son 2, 6, 7, 8, cuya suma $23 \equiv +1$ (mod. 11).

3^o. Para $p = 31$, las raíces primitivas son 3, 11, 12, 13, 17, 21, 22, 24 cuya suma $123 \equiv -1 \pmod{31}$.

Demostración. Arriba hemos demostrado (art. 55, II), que si $p-1$ es $= a^\alpha b^\beta c^\gamma$ etc. (donde a, b, c, etc. designan números primos diferentes), y A, B, C, etc. son números cualesquiera pertenecientes a los exponentes a^α, b^β, c^γ, etc., respectivamente, entonces todos los productos ABC etc. representarán raíces primitivas. También puede demostrarse fácilmente que cualquier raíz primitiva puede representarse por tal tipo de producto, y de hecho de manera única*).

De esto sigue que estos productos pueden tomarse en lugar de las raíces primitivas mismas. Pero, puesto que en estos productos conviene combinar todos los valores de A con todos los de B, etc., la suma de todos estos productos es un producto de la suma de todos los valores de A, multiplicada por la suma de todos los valores de B, multiplicada por la suma de todos los valores de C, etc., como es conocido de la teoría de combinaciones. Denótense todos los valores de A; B etc., por A, A', A", etc.; B, B', B", etc. etc., entonces la suma de todas las raíces primitivas será:

$$\equiv (A + A' + \text{ etc.})(B + B' + \text{ etc.}) \text{ etc.}$$

Ahora digo que si el exponente α es $= 1$, la suma $A + A' + A$" $+$ etc. será $\equiv -1 \pmod{p}$, pero si α es > 1, esta suma será $\equiv 0$, y de manera similar para los restantes β, γ, etc. Tan pronto como esto sea demostrado, la verdad de nuestro teorema será manifiesta. De hecho, cuando $p-1$ es divisible por algún cuadrado, alguno de los exponentes α, β, γ, etc. superará a la unidad, de donde alguno de los factores cuyo producto es congruente a la suma de todas las raíces primitivas será $\equiv 0$, y por eso también lo será el producto mismo. Pero cuando $p-1$ no puede dividirse por ningún cuadrado, todos los exponentes α, β, γ, etc. serán $= 1$, de donde la suma de todas las raíces primitivas será congruente al producto de tantos factores, cada uno de los cuales es $\equiv -1$, como cantidad de números a, b, c, etc. se tenga. Por eso la suma será $\equiv \pm 1$, según que el número de éstos sea par o impar. Ello se demuestra como sigue.

1^o. Cuando $\alpha = 1$ y A es un número perteneciente al exponente a, los restantes números que pertenecen a este exponente serán A^2, A^3, $\ldots A^{a-1}$. Pero

$$1 + A + A^2 + A^3 + \ldots + A^{a-1}$$

*) Claramente determínense los números $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, etc. de manera que $\mathfrak{a} \equiv 1 \pmod{a^\alpha}$ y $\equiv 0 \pmod{b^\beta c^\gamma}$ etc.); $\mathfrak{b} \equiv 1 \pmod{b^\beta}$ y $\equiv 0 \pmod{a^\alpha c^\gamma}$ etc.) etc. (véase art. 32), de donde será $\mathfrak{a} + \mathfrak{b} + \mathfrak{c} +$ etc. $\equiv 1 \pmod{p-1}$, (art. 19). Ahora, si cualquier raíz primitiva r se representa por el producto ABC etc., se tomará $A \equiv r^{\mathfrak{a}}$, $B \equiv r^{\mathfrak{b}}$, $C \equiv r^{\mathfrak{c}}$, etc., luego A pertenecerá al exponente a^α, B al exponente b^β, etc.; el producto de todos los números A, B, C, etc., será $\equiv r \pmod{p}$. Finalmente se ve con facilidad que A, B, C, etc., no pueden determinarse de ninguna otra manera.

es la suma de un período completo, de donde $\equiv 0$ (art. 79), por lo cual

$$A + A^2 + A^3 + \ldots + A^{a-1} \equiv -1$$

2^o. Sin embargo, cuando $\alpha > 1$ y A es un número perteneciente al exponente a^α, se tendrán los restantes números que pertenecen a este exponente, si de A^2, A^3, A^4, $\ldots A^{a^\alpha - 1}$ se suprimen A^a, A^{2a}, A^{3a}, etc., (véase art. 53). Entonces la suma de ellos será

$$\equiv 1 + A + A^2 + \ldots + A^{a^\alpha - 1} - (1 + A + A^{2a} + \ldots + A^{a^\alpha - a})$$

i.e., congruente a la diferencia de dos períodos, y por eso $\equiv 0$. *Q. E. D.*

Sobre los módulos que son potencias de números primos.

82.

Todo lo que hasta ahora hemos expuesto se ha basado en la suposición de que el módulo es un número primo. Nos queda considerar el caso donde se toma un número compuesto como módulo. Pero como aquí ni se presentan propiedades tan elegantes como en el caso anterior, ni es necesario buscar artificios sutiles para éstas, sino más bien casi todo puede extraerse por medio de una aplicación de los principios anteriores, sería superfluo y tedioso discutir todos los detalles aquí. Así que expondremos brevemente cuáles casos son comunes al caso anterior y cuales son propios.

83.

Las proposiciones de los artículos 45–48 ya fueron demostradas en general. Pero la proposición del art. 49 tiene que cambiarse como sigue:

Si f denota cuántos números son primos a m y, a la vez, menores que m, i.e., si $f = \varphi m$ (art. 38), entonces el exponente t de la potencia menor de un número dado a primo a m que es congruente a la unidad según el módulo m, será $= f$, o bien un factor de este número.

La demostración de la proposición del artículo 49 también puede valer para este caso, si se sustituyen p por m, $p-1$ por f, y los números 1, 2, 3, $\ldots p-1$, por los números a la vez menores que y primos a m. Dejamos esta tarea al lector.

Además las restantes demostraciones de las cuales hemos hablado allí (art. 50, 51) no pueden aplicarse a este caso sin mucha ambigüedad. Con respecto a las proposiciones de los artículos 52 y siguientes, nace una gran diferencia entre los módulos que son potencias de números primos y los que pueden dividirse por muchos números primos. Por lo tanto, consideraremos los módulos del género anterior por separado.

84.

Si el módulo $m = p^n$, donde p es un número primo, será $f = p^{n-1}(p-1)$ (art. 38). Ahora, si a este caso se aplican las investigaciones contenidas en los artículos 53 y 54, hechos los cambios necesarios como prescribimos en el artículo anterior, se descubrirá que todo lo que se demostró allí valdrá también en este caso, si se demostrara antes que una congruencia de la forma $x^t - 1 \equiv 0 \pmod{p^n}$ no puede tener más que t raíces diferentes. Para un módulo primo dedujimos esta verdad de las proposiciones más generales del art. 43, las cuales valen en su mayor generalidad solamente para módulos que son números primos, y por eso no debe aplicarse a este caso. No obstante demostraremos utilizando un método especial, que esta proposición es verdadera en este caso particular. Luego (sección VIII) aprenderemos a encontrarla más fácilmente.

85.

Nos proponemos demostrar este teorema:

Si e es el máximo común divisor de los números t y $p^{n-1}(p-1)$, la congruencia $x^t \equiv 1 \pmod{p^n}$ tendrá e raíces diferentes.

Sea $e = kp^\nu$ tal que k no involucre el factor p, de modo que divida al número $p-1$. Entonces la congruencia $x^t \equiv 1$, según el módulo p, tendrá k raíces diferentes denotadas A, B, C, etc., y cualquier raíz de la misma congruencia según el módulo p^n, debe ser congruente, según el módulo p, a alguno de los números A, B, C, etc. Ahora demostraremos que la congruencia $x^t \equiv 1 \pmod{p^n}$ tiene p^ν raíces congruentes a A, otras tantas a B etc., todas según el módulo p. Por esto, el número de todas las raíces será kp^ν o sea e, como hemos dicho. Para llevar a cabo esta demostración,demostraremos *primero*, que si α es una raíz congruente a A según el módulo p, también

$$\alpha + p^{n-\nu}, \quad \alpha + 2p^{n-\nu}, \quad \alpha + 3p^{n-\nu}, \quad \ldots \alpha + (p^\nu - 1)p^{n-\nu}$$

serán raíces; *segundo*, que los números congruentes a A según el módulo p diferentes de los que estén comprendidos en la forma $\alpha + hp^{n-\nu}$ (donde h denota cualquier entero) no pueden ser raíces. De donde es claro que se tendrán p^ν raíces diferentes, y no más: lo mismo tendrá que valer también para las raíces que son congruentes a cada uno de los números B, C, etc. *Tercero*, mostraremos como se puede siempre encontrar una raíz congruente a A según p.

86.

Teorema. *Si, como en el artículo anterior, t es un número divisible por p^ν pero no por $p^{\nu+1}$, tendremos:*

$$(\alpha + hp^\mu)^t - \alpha^t \equiv 0 \pmod{p^{\mu+\nu}}, \quad \text{y} \quad \equiv \alpha^{t-1} hp^\mu t \pmod{p^{\mu+\nu+1}}$$

La última parte del teorema no tiene lugar cuando $p = 2$ y a la vez $\mu = 1$.

La demostración de este teorema puede hacerse mediante el desarrollo de la potencia de un binomio, si se muestra que todos los términos después del segundo son divisibles por $p^{\mu+\nu+1}$. Sin embargo, puesto que la consideración de los denominadores de los coeficientes resulta un poco ambigua, preferimos el siguiente método.

Si suponemos *primero* $\mu > 1$ y $\nu = 1$, puesto que

$$x^t - y^t = (x-y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \text{ etc.} + y^{t-1})$$

se tendrá $$(\alpha + hp^\mu)^t - \alpha^t = hp^\mu((\alpha + hp^\mu)^{t-1} + (\alpha + hp^\mu)^{t-2}\alpha + \text{ etc.} + \alpha^{t-1})$$

Pero $$\alpha + hp^\mu \equiv \alpha \pmod{p^2}$$

por lo que cada término $(\alpha+hp^\mu)^{t-1}$, $(\alpha+hp^\mu)^{t-2}\alpha$, etc. será $\equiv \alpha^{t-1} \pmod{p^2}$, y por tanto la suma de todos será $\equiv t\alpha^{t-1} \pmod{p^2}$ o sea, será de la forma $t\alpha^{t-1} + Vp^2$, donde V denota un número cualquiera. Por eso, $(\alpha + hp^\mu)^t - \alpha^t$ será de la forma

$$\alpha^{t-1}hp^\mu t + Vhp^{\mu+2}, \quad \text{i.e.,} \quad \equiv \alpha^{t-1}hp^\mu t \pmod{p^{\mu+2}} \quad \text{y} \quad \equiv 0 \pmod{p^{\mu+1}}$$

Por lo tanto el teorema está demostrado para este caso.

Ahora, si el teorema no fuera válido para otros valores de ν, manteniendo todavía $\mu > 1$, necesariamente se presentará algún límite abajo del cual el teorema sea válido, pero más allá falso. Sea φ el menor valor de ν para el cual es falso, de donde se ve fácilmente , que si t es divisible por $p^{\varphi-1}$ pero no divisible por p^φ, el

teorema será verdadero hasta aquí, pero falso si se sustituye t por tp. Por lo tanto tenemos

$$(\alpha + hp^\mu)^t \equiv \alpha^t + \alpha^{t-1}hp^\mu t \pmod{p^{\mu+\varphi}} \quad \text{o sea} \quad = \alpha^t + \alpha^{t-1}hp^\mu t + up^{\mu+\varphi}$$

donde u denota algún número entero. Pero ya que el teorema está demostrado para $\nu = 1$, se tendrá:

$$(\alpha^t + \alpha^{t-1}hp^\mu t + up^{\mu+\varphi})^p \equiv \alpha^{tp} + \alpha^{tp-1}hp^{\mu+1}t + \alpha^{tp-t}up^{\mu+\varphi+1} \pmod{p^{\mu+\varphi+1}}$$

y por lo tanto también

$$(\alpha + hp^\mu)^{tp} \equiv \alpha^{tp} + \alpha^{tp-1}hp^\mu tp \pmod{p^{\mu+\varphi+1}}$$

i.e., el teorema también es válido si se sustituye t por tp, i.e., también para $\nu = \varphi$ contra la hipótesis. De donde es claro que el teorema será válido para todos los valores de ν.

87.

Falta el caso donde $\mu = 1$. Por medio de un método enteramente similar al que hemos aplicado en el artículo anterior, puede demostrarse sin usar el teorema binomial que

$$\begin{aligned}(\alpha + hp)^{t-1} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \pmod{p^2}\\ \alpha(\alpha + hp)^{t-2} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp\\ \alpha^2(\alpha + hp)^{t-3} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp\end{aligned}$$

etc.

de donde su suma (puesto que el número de términos $= t$) será

$$\equiv t\alpha^{t-1} + \frac{(t-1)t}{2}\alpha^{t-2}hp \pmod{p^2}$$

Sin embargo, puesto que t es divisible por p, también $\frac{(t-1)t}{2}$ será divisible por p en todos los casos, excepto en aquél donde $p = 2$, sobre el cual ya hemos informado en el artículo anterior. Pero, en los casos restantes será $\frac{(t-1)t}{2}\alpha^{t-2}hp \equiv 0 \pmod{p^2}$,

y por tanto también la suma $\equiv t\alpha^{t-1} \pmod{p^2}$ como en el artículo anterior. El resto de la demostración procede aquí del mismo modo.

Por lo tanto, concluimos en general, excepto en el único caso $p = 2$, que

$$(\alpha + hp^{\mu})^t \equiv \alpha^t \pmod{p^{\mu+\nu}}$$

y $(\alpha + hp^{\mu})^t$ *no* $\equiv \alpha^t$ para cualquier módulo que sea una potencia de p mayor que $p^{\mu+\nu}$, siempre que h no sea divisible por p, y que p^{ν} sea la potencia mayor de p que divide al número t.

De aquí, se derivan directamente las proposiciones 1 y 2, que nos habíamos propuesto demostrar: a saber,

primero, si $\alpha^t \equiv 1$, será también $(\alpha + hp^{n-\nu})^t \equiv 1 \pmod{p^n}$;

segundo, si algún número α' es congruente, según el módulo p, a A, y luego también a α, pero no congruente a α según el módulo $p^{n-\nu}$, y si satisface la congruencia $x^t \equiv 1 \pmod{p^n}$. Suponemos α' es $= \alpha + lp^{\lambda}$ de modo que l no es divisible por p, entonces será $\lambda < n - \nu$, pero entonces $(\alpha + lp^{\lambda})^t$ será congruente a α^t según el módulo $p^{\lambda+\nu}$, pero no según el módulo p^n que es una potencia mayor, por lo que α' no es una raíz de la congruencia $x^t \equiv 1$.

88.

Tercero, se debe buscar alguna raíz de la congruencia $x^t \equiv 1 \pmod{p^n}$ que sea congruente a A. Mostraremos aquí solamente cómo puede hacerse esto si ya se conoce una raíz de esta misma congruencia según el módulo p^{n-1}. Es claro que esto es suficiente, ya que podemos ir del módulo p para el cual A es una raíz, al módulo p^2 y de este a todas las potencias siguientes.

Así, sea α una raíz de la congruencia $x^t \equiv 1 \pmod{p^{n-1}}$, búsquese una raíz de la misma congruencia, según el módulo p^n. Póngase ésta $= \alpha + hp^{n-\nu-1}$, la cual debe tener esta forma según el artículo anterior (consideraremos por separado el caso donde $\nu = n - 1$ pues ν no puede ser mayor que $n - 1$). Por lo tanto, tendremos

$$(\alpha + hp^{n-\nu-1})^t \equiv 1 \pmod{p^{n-1}}$$

Pero

$$(\alpha + hp^{n-\nu-1})^t \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$$

Así, por consiguiente, si h se determina de modo que $1 \equiv \alpha^t + \alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$; o sea (puesto que por hipótesis $1 \equiv \alpha^t \pmod{p^{n-1}}$ y t es divisible por

p^ν) $\frac{\alpha^t-1}{p^{n-1}} + \alpha^{t-1}h\frac{t}{p^\nu}$ es divisible por p, tendremos la raíz buscada. Que esto se puede hacer es claro a partir de la sección anterior, puesto que hemos supuesto que aquí t no puede dividirse por una potencia de p mayor que p^ν, por lo tanto $\alpha^{t-1}\frac{t}{p^\nu}$ es primo a p.

Pero si $\nu = n-1$, i.e., t es divisible por p^{n-1} o sea también por una potencia mayor de p, cualquier valor de A que satisface a la congruencia $x^t \equiv 1$ según el módulo p, también satisfará a la misma según el módulo p^n. Pues si $t = p^{n-1}\tau$, será $t \equiv \tau \pmod{p-1}$: de donde, puesto que $A^t \equiv 1 \pmod{p}$, será también $A^\tau \equiv 1 \pmod{p}$. Ahora sea $A^\tau = 1 + hp$, tendremos $A^t = (1+hp)^{p^{n-1}} \equiv 1 \pmod{p^n}$ (art. 87).

89.

Todo lo derivado en el artículo 57 y siguientes con la ayuda del teorema que establece que la congruencia $x^t \equiv 1$ no puede tener más que t raíces diferentes, también vale para un módulo que es una potencia de un número primo. Si se les llama *raíces primitivas* a los números que pertenecen al exponente $p^{n-1}(p-1)$, es decir, en cuyos períodos aparecen todos los números no divisibles por p, entonces aquí también habrá raíces primitivas. Todo lo que antes presentamos sobre los índices y su aplicación a la resolución de la congruencia $x^t \equiv 1$, también puede aplicarse a este caso. Puesto que esto no ha presentado ninguna dificultad, sería superfluo repetir todo aquí. Además hemos mostrado cómo las raíces de la congruencia $x^t \equiv 1$, según el módulo p^n, pueden derivarse de las raíces de la misma congruencia según el módulo p. Pero todavía hay que agregar algo al caso donde una potencia del número 2 es módulo, puesto que fue excluído anteriormente.

Módulos que son potencias de 2.

90.

Si se toma alguna potencia del número 2, mayor que la segunda, como módulo, por ejemplo 2^n, la potencia 2^{n-2} de cualquier número impar es congruente a la unidad.

Por ejemplo $3^8 = 6561 \equiv 1 \pmod{32}$.

De hecho, cualquier número impar o está comprendido en la forma $1+4h$ o bien en $-1+4h$: de donde la proposición sigue directamente (teorema art. 86).

Puesto que el exponente al cual pertenece cualquier número impar, según el módulo 2^n, debe ser divisor de 2^{n-2}, pertenecerá a alguno de los números 1, 2, 4, 8, $\ldots 2^{n-2}$, entonces es fácil juzgar a cuál de ellos pertenece. Si el número propuesto $= 4h \pm 1$, y la mayor potencia de 2 que divide a h es $= m$ (que también puede ser $= 0$, cuando h es impar); entonces el exponente al cual pertenece el número propuesto será $= 2^{n-m-2}$ si $n > m+2$. Pero, si $n = 0$ o $< m+2$, el número propuesto es $\equiv \pm 1$ y pertenecerá o al exponente 1 o al exponente 2. Es claro que un número de la forma $\pm 1 + (2^{m+2}k)$ (la cual equivale a $4h \pm 1$) elevado a la potencia 2^{n-m-2}, será congruente a la unidad según el módulo 2^n, pero incongruente si es elevado a una potencia inferior del número 2, como se deduce del art. 86 con facilidad. Por lo tanto, cualquier número de la forma $8k+3$ o $8k+5$ pertenecerá al exponente 2^{n-2}.

91.

Se sigue de aquí que no se presentan *raíces primitivas* en el sentido aceptado antes por nosotros para esta expresión. Esto es, no hay números cuyos períodos comprenden todos los números menores que el módulo y primos a él. Sin embargo, se percibe fácilmente que aquí existe una analogía. De hecho, se encuentra que una potencia impar de un número de la forma $8k+3$ siempre tiene la forma $8k+3$; mientras que una potencia par siempre es de la forma $8k+1$. Por tanto, ninguna potencia puede ser de la forma $8k+5$ u $8k+7$. Puesto que el período de un número de la forma $8k+3$ consta de 2^{n-2} términos diferentes, cada uno de los cuales es o de la forma $8k+3$ o de la forma $8k+1$, y como no se dan más que 2^{n-2} números menores que el módulo, evidentemente cada número de la forma $8k+1$ u $8k+3$ es congruente, según el módulo 2^n, a alguna potencia de un número cualquiera de la forma $8k+3$. De modo similar puede demostrarse que el período de un número de la forma $8k+5$ consta de todos los números de la forma $8k+1$ y $8k+5$. Si, por lo tanto, se toma como base un número de la forma $8k+5$, se obtendrán índices reales de todos los números de la forma $8k+1$ y $8k+5$ tomados positivamente y de todos los de la forma $8k+3$ y $8k+7$ tomados negativamente. Aquí se consideran equivalentes dos índices congruentes según 2^{n-2}. De este modo, se debe interpretar nuestra Tabla I donde siempre tomamos el número 5 como base para los módulos 16, 32 y 64 (puesto que para el módulo 8 ninguna tabla es necesaria). Por ejemplo, al número 19, que es de la forma $8n+3$, y por lo tanto está tomado negativamente, le corresponde el índice 7 para el módulo 64, esto es $5^7 \equiv -19 \pmod{64}$. Pero al tomar números de las formas $8n+1$, $8n+5$ negativamente, y los números de las formas $8n+3$, $8n+7$ positivamente,

ciertos índices tendrán que considerarse imaginarios. Con la introducción de esto, el cálculo de índices puede reducirse a un algoritmo bastante simple. Pero, puesto que, si deseamos exponer esto con todo rigor, nos llevará mucho tiempo, reservamos este trabajo para otra ocasión cuando quizás intentemos profundizar la teoría de las cantidades imaginarias, la cual, a nuestro juicio, nadie ha reducido a nociones claras. Los expertos pueden encontrar este algoritmo con facilidad; los menos hábiles, sin embargo, pueden usar esta tabla si han comprendido los principios presentados arriba, de la misma manera como quienes no saben nada sobre las investigaciones modernas sobre *logaritmos* imaginarios aún usan logaritmos.

Módulos compuestos de varios primos.

92.

Según un módulo compuesto de varios primos, casi todo lo que pertenece a los residuos de las potencias puede deducirse de la teoría general de las congruencias. Pero, puesto que después enseñaremos en detalle a reducir cualquier congruencia, según un módulo compuesto de varios primos, a congruencias, de las cuales el módulo es o primo o una potencia de un primo, no nos detendremos más en esto. Solamente observamos que la bellísima propiedad que vale para los otros módulos, a saber que siempre existen números cuyo período comprende todos los números primos al módulo, aquí no vale, excepto en un único caso, cuando el módulo es el doble de un número primo, o de una potencia de un número primo. De hecho si el módulo m se reduce a la forma $A^aB^bC^c$ etc., donde A, B, C, etc. denotan números primos diferentes, y si además se denota $A^{a-1}(A-1)$ por α, $B^{b-1}(B-1)$ por β, etc., y luego z es un número primo a m; será $z^\alpha \equiv 1 \pmod{A^a}$, $z^\beta \equiv 1 \pmod{B^b}$, etc. Por tanto, si μ es el mínimo común múltiplo de los números α, β, γ, etc., será $z^\mu \equiv 1$ según todos los módulos A^a, B^b, etc., de donde también según m, que es igual al producto de aquéllos. Pero, excepto el caso donde m es el doble de un número primo o de una potencia de un número primo, el mínimo común múltiplo de los números α, β, γ, etc. es menor que su producto (puesto que los números α, β, γ, etc. no pueden ser primos entre sí, sino que tienen el divisor común 2). Por tanto, ningún período puede comprender tantos términos como números menores y primos al módulo, puesto que el número de éstos es igual al producto de α, β, γ, etc. Así, por ejemplo, para $m = 1001$ la potencia 60 de cualquier número primo a m es congruente a la unidad, pues 60 es el mínimo común múltiplo de 6, 10 y 12. El caso donde el módulo es el doble de un número primo, o el doble de una potencia de un primo es totalmente

análogo al caso donde es primo o una potencia de un primo.

93.

Ya se ha hecho mención de los escritos donde otros geómetras han hablado del argumento tratado en esta sección. Para los que desean otros detalles más amplios, mencionamos en particular los siguientes comentarios del ilustre Euler que, por su perspicacia distinguen a este hombre de los demás.

Theoremata circa residua ex divisione potestatum relicta, Comm. nov. Petr., VII p. 49 y siguientes.

Demostrationes circa residua ex divisione potestatum per numeros primos resultantia, ibid., XVIII p. 85 y siguientes.

También puede agregarse *Opusculorum analyt.* 1, disertaciones 5 y 8.

Sección Cuarta

SOBRE

LAS CONGRUENCIAS DE SEGUNDO GRADO

Residuos y no residuos cuadráticos.

94.

TEOREMA. *Al tomar un número cualquiera m como módulo, de los números* 0, 1, 2, 3 , $\ldots m-1$, *más de* $\frac{1}{2}m+1$ *no pueden ser congruentes a un cuadrado si* m *es par, ni más de* $\frac{1}{2}m+\frac{1}{2}$ *pueden serlo cuando* m *es impar.*

Demostración. Puesto que los cuadrados de números congruentes son congruentes, cualquier número que pueda ser congruente a algún cuadrado, también será congruente a algún cuadrado cuya raíz sea $< m$. Por consiguiente, basta considerar los residuos mínimos de los cuadrados 0, 1, 4, 9 , $\ldots (m-1)^2$. Pero se nota fácilmente que $(m-1)^2$ es $\equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$, etc. De aquí también, cuando m es par, los residuos mínimos de los cuadrados $(\frac{1}{2}m-1)^2$ y $(\frac{1}{2}m+1)^2$, $(\frac{1}{2}m-2)^2$ y $(\frac{1}{2}m+2)^2$, etc. serán los mismos: cuando m es impar, los cuadrados $(\frac{1}{2}m-\frac{1}{2})^2$ y $(\frac{1}{2}m+\frac{1}{2})^2$, $(\frac{1}{2}m-\frac{3}{2})^2$ y $(\frac{1}{2}m+\frac{3}{2})^2$, etc. serán congruentes. De donde es evidente que otros números no pueden ser congruentes a un cuadrado, mas que aquéllos que sean congruentes a alguno de los cuadrados 0, 1, 4, 9 , $\ldots (\frac{1}{2}m)^2$ cuando m es par; y cuando m es impar, cualquier número que sea congruente a algún cuadrado necesariamente es congruente a alguno de los números 0, 1, 4, 9 , $\ldots (\frac{1}{2}m-\frac{1}{2})^2$. Por lo tanto, en el primer caso se presentarán a lo sumo $\frac{1}{2}m+1$ residuos mínimos diferentes; en el segundo caso a lo sumo $\frac{1}{2}m+\frac{1}{2}$. *Q. E. D.*

Ejemplo. Según el módulo 13, los números 0, 1, 4, 9, 3, 12, 10 se encuentran como los residuos mínimos de los cuadrados de 0, 1, 2, 3, $\ldots 6$; después de esto

aparecen en el orden inverso 10, 12, 3 etc. Por lo tanto, si algún número no es congruente a ninguno de estos residuos mínimos, o sea, no es congruente a ninguno de 2, 5, 6, 7, 8, 11, entonces no puede ser congruente a ningún cuadrado.

Según el módulo 15 se encuentran los residuos 0, 1, 4, 9, 1, 10, 6, 4; después de esto aparecen en el orden inverso. Aquí, por lo tanto, el número de residuos que pueden ser congruentes a un cuadrado es menor que $\frac{1}{2}m + \frac{1}{2}$, puesto que son 0, 1, 4, 6, 9, 10. Pero los números 2, 3, 5, 7, 8, 11, 12, 13, 14, y los que son congruentes a alguno de éstos, no pueden ser congruentes a ningún cuadrado según el módulo 15.

95.

De esto resulta que para cualquier módulo, todos los números pueden separarse en dos clases, una de las cuales contiene los números que pueden ser congruentes a algún cuadrado, la otra contiene los que no pueden serlo. Llamaremos a los primeros *residuos cuadráticos* del número que tomamos como módulo*), y los segundos *no residuos cuadráticos,* o también, cuando no se origina ambigüedad alguna simplemente *residuos* y *no residuos.* Es claro que basta poner en clases a los números 0, 1, 2, $\ldots m-1$, puesto que todos los números congruentes deberán pertenecer a una misma clase.

Iniciaremos esta investigación con los módulos primos, lo cual deberá por consiguiente entenderse aunque no se exprese verbalmente. Hay que excluir el número primo 2: se considerarán solamente los números primos *impares.*

Cuando el módulo es un número primo, el número de residuos menores que el módulo es igual al número de no residuos menores.

96.

Al tomar un número primo p como módulo, la mitad de los números 1, 2, 3, $\ldots p-1$ *serán residuos cuadráticos, los restantes serán no residuos, i.e., se presentarán* $\frac{1}{2}(p-1)$ *residuos y otros tantos no residuos.*

---

*) En este caso, propiamente lo usamos con un sentido diferente al que hemos uasado hasta ahora. En efecto, conviene decir: r es un residuo del cuadrado a^2 según el módulo m cuando $r \equiv a^2 \pmod{m}$. Pero, por brevedad, en esta sección decimos siempre que r es un residuo cuadrático de m mismo, para no tener ninguna ambigüedad. Entonces desde ahora en adelante no usaremos la expresión *residuo* para denotar un número congruente, salvo si se trata de residuos *mínimos* donde no pueda haber duda alguna.

De hecho, se demuestra fácilmente que todos los cuadrados 1, 4, 9, $\ldots \frac{1}{4}(p-1)^2$ son incongruentes. En efecto, si pudiera ser $r^2 \equiv (r')^2 \pmod{p}$ y los números r, r' distintos y no mayores que $\frac{1}{2}(p-1)$, poniendo $r > r'$, resultaría $(r-r')(r+r')$ positivo y divisible por p. Pero cada factor $r-r'$ y $r+r'$ es menor que p, por tanto la suposición no puede valer (art. 13). Así, se tienen $\frac{1}{2}(p-1)$ residuos cuadráticos contenidos entre los números 1, 2, 3 , $\ldots p-1$; de hecho, no puede haber más de ellos puesto que al agregar el residuo 0, se producen $\frac{1}{2}(p+1)$ de ellos, y este número no puede exceder el número de todos los residuos. Por consiguiente, los restantes números serán no residuos y el número de ellos $= \frac{1}{2}(p-1)$.

Puesto que cero siempre es un residuo, lo excluimos de nuestras investigaciones, lo mismo que a los números divisibles por el módulo. Puesto que este caso es claro por sí mismo, únicamente dificultaría la simetría del teorema. Por las mismas razones también hemos excluido el módulo 2.

97.

Puesto que mucho de lo que expondremos en esta sección también podrá derivarse de los principios de las secciones anteriores, y como no es inútil estudiar a fondo la misma verdad por medio de métodos diferentes, explicaremos esta relación. Se comprende fácilmente que todos los números congruentes a un cuadrado tienen índices *pares*; mientras que los que no pueden de ningún modo ser congruentes a un cuadrado, los tienen impares. Puesto que $p-1$ es un número par, tantos índices serán pares como impares, a saber $\frac{1}{2}(p-1)$, y entonces se presentarán tantos residuos como no residuos.

Ejemplo. Para el módulo..... los residuos son

3..... 1.
5..... 1, 4.
7..... 1, 2, 4.
11..... 1, 3, 4, 5, 9.
13..... 1, 3, 4, 9, 10, 12.
17..... 1, 2, 4, 8, 9, 13, 15, 16
etc.

y el resto de los números menores que el módulo son no residuos.

La cuestión de si un número compuesto es un residuo o un no residuo de un número primo dado depende de la naturaleza de los factores.

98.

TEOREMA. *El producto de dos residuos cuadráticos de un número primo p es un residuo; el producto de un residuo con un no residuo es un no residuo; finalmente, el producto de dos no residuos es un residuo.*

Demostración. I. Sean A y B los residuos resultantes de los cuadrados a^2 y b^2 o sea $A \equiv a^2, B \equiv b^2$. El producto AB será congruente al cuadrado del número ab, i.e., es un residuo.

II. Cuando A es un residuo, por ejemplo $\equiv a^2$, pero B es un no residuo, AB será un no residuo. Si fuera un residuo, póngase $AB \equiv k^2$, y sea el valor de la expresión $\frac{k}{a} \pmod{p} \equiv b$; así tendríamos $a^2B \equiv a^2b^2$, de donde $B \equiv b^2$, i.e., B es un residuo, contrariamente a la hipótesis.

Otra demostración. Entre los números 1, 2, 3 , $\ldots p-1$ (el número de ellos $= \frac{1}{2}(p-1)$), multiplíquense por A todos los que sean residuos. Todos los productos serán residuos cuadráticos, y ciertamente todos serán incongruentes. Ahora, si se multiplica el no residuo B por A, el producto no será congruente a ninguno de los productos que ya se tienen; por lo tanto si fuera un residuo, se tendrían $\frac{1}{2}(p+1)$ residuos incongruentes, entre los cuales todavía no está el residuo 0, contrariamente al art. 96.

III. Sean A y B no residuos. Entre los números 1, 2, 3 , $\ldots p-1$, multiplíquense por A todos los que sean residuos. Se tendrán $\frac{1}{2}(p-1)$ no residuos incongruentes entre sí (II); ahora el producto AB no puede ser congruente a ninguno de ellos. Entonces, si fuera un no residuo, se tendrían $\frac{1}{2}(p+1)$ no residuos incongruentes entre sí, contra el art. 96. Por lo tanto el producto etc. *Q. E. D.*

Estos teoremas pueden ser derivados más fácilmente de los principios de la sección anterior. De hecho, puesto que los índices de los residuos siempre son pares, y los índices de los no residuos impares, el índice del producto de dos residuos o de dos no residuos será par, de donde el producto mismo será un residuo. Por el contrario, el índice del producto de un residuo y un no residuo será impar y, por lo tanto, el producto mismo un no residuo.

Cualquier método de demostración también puede aplicarse para estos teoremas: *el valor de la expresión* $\frac{a}{b} \pmod{p}$ *será un residuo cuando los números a y b sean a la vez residuos o a la vez no residuos; al contrario, será un no residuo cuando uno de los números a o b sea un residuo y el otro un no residuo.* También pueden obtenerse al aplicar los teoremas precedentes.

99.

En general, el producto de factores cualesquiera es un residuo ya sea cuando todos los factores son residuos o cuando todos son no residuos y el número de ellos es par. Pero cuando el número de los no residuos que quedan entre los factores es impar, el producto será un no residuo. Así puede decidirse fácilmente si un número compuesto es residuo o no, si de algún modo se conoce cada uno de sus factores. Por lo tanto, hemos incluido solamente los números primos en la tabla II. Esta es la organización de la tabla. En la orilla se han colocado los módulos*), con los números primos consecutivos arriba. Cuando uno de éstos es un residuo de algún módulo, se coloca un guión en el espacio correspondiente a los dos, pero cuando el número primo es un no residuo del módulo, el espacio correspondiente queda en blanco.

Sobre los módulos que son numeros compuestos.

100.

Antes de proceder a temas más difíciles, debemos agregar algo acerca de los módulos no primos.

Si se toma como módulo alguna potencia p^n del número primo p (donde suponemos que p no es 2) la mitad de todos los números no divisibles por p y menores que el módulo serán residuos, la otra mitad será no residuos, i.e., el número de cada uno $= \frac{1}{2}(p-1)p^{n-1}$.

De hecho, si r es un residuo, será congruente a algún cuadrado cuya raíz no supera la mitad del módulo, véase art. 94. Ahora se nota fácilmente que se presentan $\frac{1}{2}(p-1)p^{n-1}$ números menores que la mitad del módulo y no divisibles por p. Así, falta demostrar que los cuadrados de todos estos números son incongruentes, o sea producen residuos cuadráticos diferentes. Si los cuadrados de dos números a y b no divisibles por p y menores que la mitad del módulo fueran congruentes, tendríamos $a^2 - b^2$ o sea $(a-b)(a+b)$ divisible por p^n (suponemos que $a > b$). Pero esto no puede suceder a menos que, o bien uno de los números $a-b, a+b$ sea divisible por p^n, lo que no puede ser, puesto que los dos son $< p^n$; o bien uno por p^m y el otro por p^{n-m}, i.e., ambos por p. Pero esto tampoco puede suceder. En efecto, es claro que la suma y diferencia de $2a$ y $2b$ también serían divisibles por p, de donde también a y b, contrariamente a la hipótesis.— De esto se sigue, finalmente, que entre los números no divisibles por p y menores que el módulo se presentan $\frac{1}{2}(p-1)p^n$ residuos;

*) Pronto mostraremos cómo podemos tratar con los módulos compuestos también.

los restantes, que son la misma cantidad, son no residuos. Q.E.D.— Este teorema también puede derivarse de las consideraciones de los índices tal como en el art. 97.

101.

Cualquier número no divisible por p, que es un residuo de p, también será un residuo de p^n; pero si es un no residuo de p, también será un no residuo de p^n.

La última parte de esta proposición es muy clara. Si la primera parte fuera falsa, entre los números menores que p^n y a la vez no divisibles por p, habría más residuos de p que de p^n, i.e., más de $\frac{1}{2}p^{n-1}(p-1)$. Pero, puede verse con facilidad que el número de residuos del número p entre esos números es precisamente $= \frac{1}{2}p^{n-1}(p-1)$.

Es igualmente fácil encontrar explícitamente un cuadrado congruente, según el módulo p^n, a un residuo dado, si se tiene el cuadrado congruente a este residuo según el módulo p.

En efecto, si se tiene un cuadrado a^2 que es congruente al residuo dado A según el módulo p^μ, se puede encontrar un cuadrado congruente a A según el módulo p^ν (donde se supone $\nu > \mu$ e $= $ ó $< 2\mu$) de la siguiente manera. Póngase la raíz del cuadrado deseado $= \pm a + xp^\mu$. Se ve fácilmente que debe tener esta forma, y debe ser $a^2 \equiv \pm 2axp^\mu + x^2p^{2\mu} \equiv A \pmod{p^\nu}$, o sea, puesto que $2\mu > \nu$, $A - a^2 \equiv \pm 2axp^\mu \pmod{p^\nu}$. Si $A - a^2 = p^\mu d$, x será un valor de la expresión $\pm\frac{d}{2a} \pmod{p^{\nu-\mu}}$, que es equivalente a $\pm\frac{A-a^2}{2ap^\mu} \pmod{p^\nu}$.

Por lo tanto, dado un cuadrado congruente a A según el módulo p, se deduce de allí un cuadrado congruente a A según el módulo p^2; de aquí podemos ascender a p^4, de allí a p^8 etc.

Ejemplo. Propuesto el residuo 6 que es congruente al cuadrado 1 según el módulo 5, encontramos que es congruente al cuadrado 9^2 según 25, congruente a 16^2 según 125, etc.

102.

Con respecto a los números divisibles por p, es claro que sus cuadrados serán divisibles por p^2, de donde todos los números divisibles por p pero no por p^2 serán no residuos de p^n. En general, si se propone un número p^kA, donde A no es divisible por p, podemos distinguir los siguientes casos:

1) Cuando $k =$ ó $> n$, tendremos $p^k A \equiv 0 \pmod{p^n}$, i.e., un residuo.

2) Cuando $k < n$ e impar, $p^k A$ será un no residuo.

De hecho, si tuvieramos $p^k A = p^{2\chi+1} A \equiv s^2 \pmod{p^n}$, s^2 sería divisible por $p^{2\chi+1}$ y éste únicamente podría ser el caso si s fuera divisible por $p^{\chi+1}$. Entonces, también s^2 será divisible por $p^{2\chi+2}$ y así también (puesto que en realidad $2\chi + 2$ no es mayor que n) $p^k A$ i.e., $p^{2\chi+1} A$; o sea, A es divisible por p, contrariamente a la hipótesis.

3) Cuando $k < n$ y par. Entonces $p^k A$ será un residuo o un no residuo de p^n, según que A sea un residuo o un no residuo de p. De hecho, cuando A es un residuo de p, será también un residuo de p^{n-k}. Suponiendo que $A \equiv a^2 \pmod{p^{n-k}}$, obtendremos que $Ap^k \equiv a^2 p^k \pmod{p^n}$ y que $a^2 p^k$ es un cuadrado. Pero, cuando A es un no residuo de p, $p^k A$ no puede ser un residuo de p^n. De hecho, si $p^k A \equiv a^2 \pmod{p^n}$, necesariamente a^2 será divisible por p^k. El cociente será un cuadrado congruente a A según el módulo p^{n-k}, de donde también según el módulo p, contrariamente a la hipótesis.

103.

Puesto que hemos excluido el caso $p = 2$, hay que decir algo sobre él. Cuando el número 2 es el módulo, cualquier número será un residuo y ninguno será un no residuo. Pero cuando 4 es el módulo, todos los números impares de la forma $4k + 1$ serán residuos, mientras que todos los de la forma $4k + 3$ serán no residuos. Finalmente, cuando 8 o una potencia mayor del número 2 es el módulo, todos los números impares de la forma $8k + 1$ serán residuos, pero los restantes que son de las formas $8k+3$, $8k+5$, y $8k+7$ serán no residuos. La última parte de esta proposición es clara porque el cuadrado de cualquier número impar, sea bien de la forma $4k + 1$, o bien de la forma $4k - 1$, será de la forma $8k + 1$. La primera parte la demostramos a continuación:

1) Si la suma o diferencia de dos números es divisible por 2^{n-1}, los cuadrados de dichos números serán congruentes según el módulo 2^n. Pues, si se pone uno de ellos $= a$, el otro será de la forma $2^{n-1}h \pm a$, cuyo cuadrado es $\equiv a^2 \pmod{2^n}$.

2) Cualquier número impar que es un residuo cuadrático de 2^n, será congruente a algún cuadrado cuya raíz es un número impar y $< 2^{n-2}$. Sea pues a^2 cualquier cuadrado al cual el número es congruente y sea el número $a \equiv \pm\alpha \pmod{2^{n-1}}$ de manera que α no supere la mitad del módulo (art. 4). Entonces tendremos $a^2 \equiv \alpha^2$,

y el número propuesto será también $\equiv \alpha^2$. Pero entonces es claro que tanto a como α serán impares y $\alpha < 2^{n-2}$.

3) Los cuadrados de todos los números impares menores que 2^{n-2} serán incongruentes según 2^n. De hecho, si r y s son dos números tales, cuyos cuadrados fueran congruentes según 2^n, $(r-s)(r+s)$ sería divisible por 2^n (suponiendo que $r > s$). Pero se ve fácilmente que los números $r-s$ y $r+s$, no pueden ser divisibles a la vez por 4; por lo tanto si uno es divisible sólo por 2, el otro deberá ser divisible por 2^{n-1} para que el producto sea divisible por 2^n. Q.E.A., puesto que cada uno es $< 2^{n-2}$.

4) Si finalmente se reducen estos cuadrados a sus *residuos mínimos positivos,* se obtendrán 2^{n-3} residuos cuadráticos diferentes menores que el módulo*) y cada uno será de la forma $8k+1$. Sin embargo, como existen precisamente 2^{n-3} números de la forma $8k+1$ menores que el módulo, todos estos números deben ser residuos. *Q. E. D.*

Para encontrar un cuadrado congruente a un número dado de la forma $8k+1$ según el módulo 2^n, puede emplearse un método como en el art. 101; véase también art. 88. — Finalmente, lo mismo que hemos expuesto en general en el art. 102 vale para los números pares.

104.

Si A es un residuo de p^n, se deriva con facilidad de lo anterior lo siguiente acerca del número de valores diferentes (i.e., de los incongruentes según el módulo) que admiten una expresión como $V = \sqrt{A} \pmod{p^n}$. (Suponemos, como antes, que el número p es primo y, por brevedad, incluimos aquí el caso $n = 1$).

I. Si A no es divisible por p, V tiene un valor *único* para $p = 2$, $n = 1$, a saber $V = 1$; *dos* valores cuando p es impar, o cuando $p = 2$, $n = 2$, a saber, al poner uno de ellos $\equiv v$, el otro será $\equiv -v$; *cuatro* valores para $p = 2$, $n > 2$, en efecto, al poner uno de ellos $\equiv v$, los restantes serán $\equiv -v$, $2^{n-1} + v$, $2^{n-1} - v$.

II. Si A es divisible por p, pero no por p^n, sea $p^{2\mu}$ la potencia más alta de p que divide a A, (de hecho, es claro que este exponente deberá ser par) y tendremos $A = ap^{2\mu}$. Entonces, es claro que todos los valores de V serán divisibles por p^μ, y los cocientes que resultan de la división serán valores de la expresión $V' = \sqrt{a} \pmod{p^{n-2\mu}}$; de donde producirán todos los valores diferentes de V, al multiplicar

*) Porque el número de enteros impares menores que 2^{n-2} es 2^{n-3}.

todos los valores de la expresión V' situados entre 0 y $p^{n-\mu}$ por p^μ. Por lo tanto se representarán por

$$vp^\mu,\ vp^\mu + p^{n-\mu},\ vp^\mu + 2p^{n-\mu},\ \ldots\ vp^\mu + (p^\mu - 1)p^{n-\mu}$$

donde el valor indeterminado v representa todos los valores *diferentes* de la expresión V', de modo que el número de ellos será p^μ, $2p^\mu$, o $4p^\mu$, según que el número de valores de V' (por el caso I) sea 1, 2 o 4.

III. Si A es divisible por p^n, se ve fácilmente, al colocar $n = 2m$ ó $= 2m-1$, según sea par o impar, que todos los números divisibles por p^m son valores de V y no hay otros. Por consiguiente todos los valores diferentes serán 0, p^m, $2p^m$, $\ldots (p^{n-m} - 1)p^m$ y el número de ellos es p^{n-m}.

105.

Falta el caso donde el módulo m está compuesto de varios números primos. Sea $m = abc\ldots$ donde a, b, c, etc. denotan números primos diferentes o potencias de números primos diferentes. Es claro aquí que si n es un residuo de m, también será n un residuo de cada uno de los números a, b, c, etc., de donde n ciertamente será un no residuo de m, si es un no residuo de alguno de los números a, b, c, etc. Y vice-versa: si n es un residuo de cada uno de a, b, c, etc., también será un residuo del producto m. Pues, al suponer que $n \equiv A^2$, B^2, C^2, etc., mod. a, b, c, etc. respectivamente, es claro, si se deriva un número N congruente a A, B, C, etc. según el módulo a, b, c, etc. respectivamente (art. 32), se tendrá $n \equiv N^2$ según todos estos módulos y también según su producto m. Se nota fácilmente cómo de una combinación de *cualquier* valor de A, es decir $\sqrt{n}$ (mod. a), con *cualquier* valor de B, y con *cualquier* valor de C etc. resulta un valor de N, o de la expresión $\sqrt{n}$ (mod. m). Además, diferentes combinaciones del producto dan diferentes valores de N y todas las combinaciones dan todos los valores de N. El número de todos los diferentes valores de N será igual al producto de los números de valores de A, B, C, etc. que enseñamos a determinar en el artículo anterior. — Además, es claro que si un valor de la expresión $\sqrt{n}$ (mod. m) o de N es conocido, a la vez será éste un valor de A, B, C, etc. Puesto que según el artículo anterior, pueden deducirse todos los restantes valores de estas cantidades, sigue fácilmente que, de un valor de N, pueden obtenerse todos los restantes.

Ejemplo. Sea el módulo 315, del cual se desea saber si 46 es residuo o no residuo. Los divisores primos del número 315 son 3, 5, y 7; y el número 46 es un residuo de cada uno y por tanto también residuo de 315. Además, puesto que $46 \equiv 1$, y $\equiv 64 \pmod 9$; $\equiv 1$ y $\equiv 16 \pmod 5$; $\equiv 4$ y $\equiv 25 \pmod 7$, se encuentran las raíces de los cuadrados a los que 46 es congruente según el módulo 315, que son los números 19, 29, 44, 89, 226, 271, 289, 296.

Criterio general sobre si un número dado es un residuo de un número primo dado.

106.

De lo anterior se concluye: si sólo se puede decidir si un *número primo* dado es un residuo o un no residuo de un *número primo dado,* todos los casos restantes pueden reducirse a esto. Por lo tanto debemos dirigir todos nuestros estudios a investigar criterios verdaderos para este caso. Antes de llevar a cabo esta investigación presentaremos un criterio derivado de la sección anterior, el cual en la práctica casi nunca tiene utilidad, pero que por su simplicidad y generalidad debe mencionarse.

Cualquier número A no divisible por un número primo $2m+1$ es un residuo o no residuo de este número primo según $A^m \equiv +1$ o $\equiv -1 \pmod{2m+1}$.

Sea pues a el índice del número A para el módulo $2m+1$ en un sistema cualquiera; a será par cuando A es un residuo de $2m+1$, e impar cuando es un no residuo. Pero, el índice del número A^m será ma, i.e., $\equiv 0$ o $\equiv m \pmod{2m}$ según a sea par o impar. De aquí finalmente en el primer caso A^m será $\equiv +1$, pero en el siguiente $\equiv -1 \pmod{2m+1}$. Véase artículos 57 y 62.

Ejemplo. 3 es un residuo de 13 ya que $3^6 \equiv 1 \pmod{13}$, pero 2 es un no residuo de 13, puesto que $2^6 \equiv -1 \pmod{13}$.

Tan pronto como los números por examinarse sean moderadamente grandes, este criterio será completamente inútil a causa de la inmensidad del cálculo.

Investigaciones sobre los números primos cuyos residuos o no residuos sean números dados.

107.

Dado un módulo, es muy fácil caracterizar todos los números que son residuos o no residuos. Es claro: si se coloca este número $= m$, deben determinarse los cuadrados cuyas raíces no superan la mitad de m, o también números congruentes a

estos cuadrados según m (en la práctica se presentan métodos más fáciles). Entonces, todos los números congruentes a alguno de éstos según m serán residuos de m, y todos los números no congruentes a ninguno de ellos serán no residuos. — Pero la situación inversa, *propuesto algún número, asignar todos los números, de los cuales aquél sea un residuo o no residuo,* es un obstáculo mucho más grande. Este problema, de cuya solución depende lo que hemos propuesto en el artículo precedente, será estudiado a fondo en lo siguiente, comenzando con los casos más sencillos.

Residuo −1.

108.

TEOREMA. -1 *es un residuo cuadrático de todos los números primos de la forma* $4n+1$*, pero es un no residuo de todos los números primos de la forma* $4n+3$.

Ejemplo. -1 es un residuo de los números 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc. originado de los cuadrados de los números 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22, etc. respectivamente; al contrario, es un no residuo de los números 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, etc.

Ya hemos mencionado este teorema en el artículo 64. La demostración se obtiene fácilmente del art. 106. Pues, para un número primo de la forma $4n+1$ se tiene $(-1)^{2n} \equiv 1$, pero para un número de la forma $4n+3$ se tiene $(-1)^{2n+1} \equiv -1$. Esta demostración concuerda con la del artículo mencionado. Sin embargo, por la elegancia y utilidad del teorema, mostraremos otra solución.

109.

Denotamos al conjunto de todos los residuos del número primo p, menores que p, excluyendo el residuo 0, por la letra C. Puesto que el número de estos residuos siempre será $= \frac{p-1}{2}$, es claro que será par si p es de la forma $4n+1$, pero impar si p es de la forma $4n+3$. Por semejanza con el art. 77 donde se hablaba sobre números en general, se llaman *residuos asociados* a dos números cuyo producto $\equiv 1 \pmod{p}$. De hecho, es claro que si r es un residuo, también $\frac{1}{r} \pmod{p}$ será un residuo. Puesto que un mismo residuo no puede tener más asociados entre los residuos C, es evidente que todos los residuos C pueden distribuirse en clases, de las cuales cada una contenga dos residuos asociados. Ahora, es claro, si no se presenta ningún residuo que no esté asociado a sí mismo, i.e., si cada clase contuviera dos residuos *diferentes,* el número de todos los residuos sería el doble del número de todas las clases. Pero, si se presenta

algunos residuos que son sus propios asociados, i.e., algunas clases que contienen un residuo único, o, si se quiere, contienen el mismo residuo dos veces, y si se pone el número de estas clases $= a$, y el número de las restantes $= b$, entonces el número de todos los residuos C será $= a + 2b$. De donde, cuando p es de la forma $4n + 1$, a será un número par. Cuando p es de la forma $4n + 3$, a será impar. Pero, no hay números menores que p, salvo 1 y $p - 1$, que puedan estar asociados consigo mismos (véase art. 77). En el primer caso, 1 está entre los residuos; por lo tanto $p - 1$ (ó -1 que vale lo mismo) debe ser un residuo, pero en el segundo caso, debe ser un no residuo. Pues, en un caso será $a = 1$, y en el otro $= 2$, lo cual es imposible.

110.

También esta demostración se debe al ilustre Euler, quien también encontró por primera vez el método anterior (véase *Opuscula Analytica*, T.1, *p.* 135). Con facilidad, se verá que ella está basada en principios semejantes a los de nuestra segunda demostración del teorema de Wilson (art. 77). Pero si suponemos este teorema, la demostración podría simplificarse mucho. Es claro que entre los números 1, 2, 3 , $\ldots p-1$ habrá $\frac{p-1}{2}$ residuos cuadráticos de p y otros tantos no residuos. Por lo que el número de residuos será par cuando p es de la forma $4n + 1$; impar, cuando p es de la forma $4n + 3$. De aquí concluimos que el producto de todos los números 1, 2, 3, , $\ldots p - 1$ será un residuo en el primer caso, un no residuo en el otro caso (art. 99). Pero este producto siempre $\equiv -1 \pmod{p}$; de donde -1 es un residuo en el primer caso y en el segundo caso será un no residuo.

111.

Así, si r es un residuo de algún número primo de la forma $4n + 1$, también $-r$ será un residuo de este primo; todos los no residuos de tal número se mantendrán como no residuos, aunque se cambie el signo*). Lo contrario vale para los números primos de la forma $4n + 3$, cuyos residuos, cuando se cambia de signo, se convierten en no residuos y viceversa (véase art. 98).

Además de lo que precede, es fácil derivar una regla general: -1 *es un residuo de todos los números no divisibles ni por* 4 *ni por ningún número primo de la forma* $4n + 3$. *El es un no residuo de todos los restantes.* Véanse art. 103 y 105.

*) Por eso, cuando hablamos de cualquier número, sea un residuo o no residuo de un número de la forma $4n + 1$, podremos ignorar completamente el signo o bien emplear el signo doble $\pm$.

Residuos +2 y −2.

112.

Llegamos a los residuos +2 y −2.

Si de la tabla II recogemos todo número primo del cual +2 es un residuo, tendremos: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Es fácil observar que entre estos números ninguno es de la forma $8n + 3$ ni $8n + 5$.

Veamos si de esta inducción puede hacerse una certidumbre.

Notamos primero que todo número compuesto de la forma $8n + 3$ u $8n + 5$ necesariamente involucra un factor primo de una de las dos formas $8n + 3$ u $8n + 5$. Pues, es claro que números primos de la forma $8n + 1$ u $8n + 7$ pueden formar únicamente números que son de la forma $8n + 1$ u $8n + 7$. Por lo tanto, si nuestra inducción es cierta en general, no se presentará ningún número de la forma $8n + 3$ u $8n + 5$ cuyo residuo sea +2. Pero, ciertamente, no existe ningún número de esta forma menor que 100 del cual +2 es un residuo. Sin embargo, si se encuentran tales números más allá de este límite, sea el menor de todos ellos $= t$. Así pues t será o de la forma $8n + 3$ o de la forma $8n + 5$; +2 será un residuo de t, pero un no residuo de todos los números semejantes menores que t. Si se pone $2 \equiv a^2 \pmod{t}$, siempre a podrá tomarse como impar y a la vez $< t$, (puesto que a tendrá al menos dos valores positivos menores que t cuya suma $= t$, de los cuales uno es par y el otro impar, véanse art. 104 y 105). Por la misma razón, sea $a^2 = 2 + tu$, es decir $tu = a^2 - 2$, a^2 será de la forma $8n + 1$, tu por lo tanto de la forma $8n - 1$, y así u será de la forma $8n + 3$ u $8n + 5$ según sea t de la segunda forma o de la primera forma. Pero, de la ecuación $a^2 = 2 + tu$ se sigue también que $2 \equiv a^2 \pmod{u}$, i.e., 2 también será un residuo de u. Pero con facilidad se percibe que $u < t$, de donde t no es el número menor en nuestra inducción, contrariamente a la hipótesis. Así se sigue claramente que lo que habíamos encontrado por inducción para el caso general es verdadero.

Al combinar esto con la proposición del art. 111, encontramos los siguientes teoremas:

I. *+2 será un no residuo y −2 un residuo de todos los números primos de la forma* $8n + 3$.

II. *Tanto +2 como −2 serán no residuos de todos los números primos de la forma* $8n + 5$.

113.

Mediante una inducción semejante a la de la tabla II se encuentran que −2

es un residuo de los siguientes números primos: 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97*). Puesto que ningúno de ellos es de la forma $8n+5$ u $8n+7$, investigaremos entonces si es que esta inducción puede tener la fuerza de un teorema general. Se demuestra de modo semejante al artículo anterior que todo número compuesto de la forma $8n+5$ u $8n+7$ involucra un factor primo de la forma $8n+5$ u $8n+7$, de tal manera que, si nuestra generalización es cierta, -2 no puede ser un residuo de ningún número de la forma $8n+5$ u $8n+7$. Pero si tales números existen, sea el menor de ellos $= t$ y tendremos $-2 = a^2 - tu$. Si como antes se toma a impar y menor que t, u será de la forma $8n+5$ u $8n+7$ según que t sea de la forma $8n+7$ u $8n+5$. Pero de $a^2+2 = tu$ y $a < t$ podrá derivarse fácilmente también que u será menor que t. Finalmente, -2 será un residuo de u, i.e., t no será el menor número de los que -2 es residuo, contradiciendo la hipótesis de nuestra inducción. Por lo que -2 necesariamente es un no residuo de todos los números de las formas $8n+5$ y $8n+7$.

Al combinarse esto con la proposición del art. 111, se obtienen estos teoremas:

I. *Tanto* -2 *como* $+2$ *son no residuos de todos los números primos* $8n+5$, tal como vimos en el artículo anterior.

II. -2 *es un no residuo y* $+2$ *es un residuo de todos los números primos de la forma* $8n+7$.

Además, en ambas demostraciones habríamos podido tomar a como un número par. Pero entonces, habríamos tenido que distinguir el caso donde a fuera de la forma $4n+2$ del caso en donde a fuera de la forma $4n$. El desarrollo procede tal como antes sin dificultad alguna.

114.

Falta el caso en que el número primo es de la forma $8n+1$. Pero esto no se puede resolver por el método anterior y exige artificios muy particulares.

Sea a cualquier raíz primitiva para el módulo $8n+1$, por lo que $a^{4n} \equiv -1 \pmod{8n+1}$ (art. 62). Tal congruencia puede también expresarse en la forma $(a^{2n}+1)^2 \equiv 2a^{2n} \pmod{8n+1}$, o bien por $(a^{2n}-1)^2 \equiv -2a^{2n}$. De donde se sigue que tanto $2a^{2n}$ como $-2a^{2n}$ son residuos de $8n+1$; pero puesto que a^{2n} es un cuadrado no divisible por el módulo, es claro también que tanto $+2$ como -2 serán residuos (art. 98).

---

*) Esto es considerando a -2 como producto de $+2$ y -1. Véase art. 111.

115.

No será inútil agregar ahora otra demostración de este teorema. Esta guarda una relación con la anterior como la segunda demostración (art. 109) del teorema del art. 108 con la primera (art. 108). Los peritos notarán fácilmente que las dos demostraciones no son tan diferentes como quizás aparentan al principio, tanto en el primer caso como en el segundo.

I. Entre los números 1, 2, 3, ... $4m$ menores que un módulo primo cualquiera de la forma $4m + 1$, aparecerán m números que pueden ser congruentes a un bicuadrado, mientras que los restantes $3m$ no podrán ser congruentes.

Esto se deriva fácilmente de los principios de la sección anterior, pero también sin éstos la demostración es fácil. En efecto, hemos demostrado que para tal módulo -1 siempre es un residuo cuadrático. Sea así $f^2 \equiv -1$. Es claro que si z es un número cualquiera no divisible por el módulo, los bicuadrados de los cuatro números $+z$, $-z$, $+fz$, $-fz$ (se percibe con facilidad que dos cualesquiera de ellos son incongruentes) son congruentes entre sí. Además, es claro que el bicuadrado de un número cualquiera que no es congruente a ninguno de estos cuatro no puede ser congruente a los bicuadrados de ellos (en efecto, la congruencia $x^4 \equiv z^4$, la cual es de cuarto grado, tendría más de cuatro raíces, contrariamente al art. 43). De esto se deduce fácilmente que todos los números 1, 2, 3, ... $4m$ dan lugar a m bicuadrados no congruentes y que entre estos mismos números se encontrarán m números congruentes a éstos, mientras que los restantes no podrán ser congruentes a ningún bicuadrado.

II. Según un módulo primo de la forma $8n + 1$, -1 podrá ser congruente a un bicuadrado (-1 será un *residuo bicuadrático* de este número primo).

De hecho, el número de residuos bicuadráticos menores que $8n+1$ (excluyendo a cero) será $= 2n$, i.e., par. Además, se muestra fácilmente que, si r es un residuo bicuadrático de $8n + 1$, también será un residuo el valor de la expresión $\frac{1}{r} \pmod{8n + 1}$. De esto: todos los residuos bicuadráticos podrán distribuirse en clases de modo semejante a como los distribuimos en el art. 109. La parte restante de la demostración procede exactamente de la misma manera que allí.

III. Ahora, sea $g^4 \equiv -1$ y h un valor de la expresión $\frac{1}{g} \pmod{8n + 1}$. Por tanto, será

$$(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2$$

(ya que $gh \equiv 1$). Pero $g^4 \equiv -1$ así que $-h^2 \equiv g^4h^2 \equiv g^2$ de donde $g^2 + h^2 \equiv 0$ y $(g \pm h)^2 \equiv \pm 2$, i.e., tanto $+2$ como -2 son residuos cuadráticos de $8n + 1$. *Q. E. D.*

116.

La siguiente regla general se deduce fácilmente de lo anterior: $+2$ *es un residuo de cualquier número que no puede dividirse ni por* 4 *ni por ningún número primo de la forma* $8n+3$ *u* $8n+5$*, pero es un no residuo de los restantes* (por ejemplo, de todos los números de la forma $8n+3$ y $8n+5$ tanto primos como compuestos).

-2 *es un residuo de cualquier número que no puede dividirse ni por* 4*, ni por ningún primo de la forma* $8n+5$ *u* $8n+7$*; pero de todos los restantes es un no residuo.*

El sagaz Fermat también conoció estos teoremas tan elegantes (*Op. Mathem.,* p. 168). Aunque afirmó tener una demostración, nunca la presentó. Luego, el ilustre Euler la buscó siempre en vano, pero fue el ilustre Lagrange quién logró la primera demostración rigurosa, (*Nouv. Mém. de l'Ac. de Berlin, 1775,* p. 349, 351). El ilustre Euler parece no haberla visto cuando escribió su disertación conservada en su *Opusc. Analyt.,* (T. I., p. 259).

Residuos $+3$ *y* -3.

117.

Pasamos a los residuos $+3$ y -3. Iniciamos con el segundo de ellos.

De la tabla II encontramos que -3 es un residuo de estos números primos: 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, entre los cuales no se encuentra ninguno de la forma $6n+5$. Demostramos de la manera siguiente que tampoco afuera de los límites de la tabla existen primos de esta forma, de los cuales -3 es un residuo. Primero, es claro que cualquier número compuesto de la forma $6n+5$ involucra necesariamente algún factor primo de la misma forma. Por lo tanto, hasta el punto en que no exista ningún número primo de la forma $6n+5$ cuyo residuo sea -3, tampoco existirá un número compuesto con esta propiedad. Si tales números existen fuera de los límites de nuestra tabla, sea el menor de todos $= t$ y sea $-3 = a^2 - tu$. Por lo tanto, si a se toma par y menor que t, tendremos $u < t$ y -3 será un residuo de u. Pero cuando a es de la forma $6n \pm 2$, tu será de la forma $6n+1$, de donde u es de la forma $6n+5$. Q. E. A., puesto que hemos supuesto que t es el menor de los números contrariamente a nuestra inducción. Pero cuando a es de la forma $6n$, será tu de la forma $36n+3$, así que $\frac{1}{3}tu$ será de la forma $12n+1$, por lo que $\frac{1}{3}u$ será de la forma $6n+5$; pero es claro que -3 será también un residuo de $\frac{1}{3}u$ aunque $\frac{1}{3}u < t$, Q. E. A. Por lo tanto es claro que -3 no puede ser un residuo de ningún número de la forma $6n+5$.

Ya que cualquier número de la forma $6n+5$ está contenido necesariamente entre aquéllos de la forma $12n+5$ o $12n+11$ y puesto que la primera es de la forma

$4n+1$ y la segunda de la forma $4n+3$, se tienen los siguientes teoremas:

I. *Tanto* -3 *como* $+3$ *son no residuos de cualquier número primo de la forma* $12n+5$.

II. -3 *es un no residuo y* $+3$ *es un residuo de cualquier número primo de la forma* $12n+11$.

118.

Los números que encontramos en la tabla II y que tienen residuo $+3$ son: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97; entre ellos, ninguno es de la forma $12n+5$ o $12n+7$. Puede comprobarse exactamente como en los artículos 112, 113 y 117 que no existe ningún número de las formas $12n+5$ ni $12n+7$ cuyo residuo sea $+3$, por lo que suprimimos este desarrollo. Combinando estos resultados con los del art. 111 tenemos los siguentes teoremas:

I. *Tanto* $+3$ *como* -3 *son no residuos de cualquier número primo de la forma* $12n+5$ (tal como ya encontramos en el artículo anterior).

II. $+3$ *es un no residuo y* -3 *es un residuo de cualquier número primo de la forma* $12n+7$.

119.

Mediante este método, no se puede descubrir nada con respecto a los números de la forma $12n+1$, por lo que exigen artificios particulares. Por una inducción se deduce fácilmente que $+3$ y -3 son residuos de todos los números primos de esta forma. Pero, es claro que debe demostrarse solamente que -3 es un residuo de tales números, ya que necesariamente $+3$ será un residuo (art. 111). Sin embargo demostraremos más generalmente que -3 es un residuo de cualquier número primo de la forma $3n+1$.

Sea p un primo de este tipo y a un número que, para el módulo p, pertenece al exponente 3 (los cuales existen por el art. 54, ya que 3 es divisor de $p-1$). Por eso será $a^3 \equiv 1 \pmod{p}$, i.e., a^3-1 o sea $(a^2+a+1)(a-1)$ será divisible por p. Pero es claro que a no puede ser $\equiv 1 \pmod{p}$, ya que 1 pertenece al exponente 1, por lo que $a-1$ no será divisible por p, pero a^2+a+1 lo será, y de allí también $4a^2+4a+4$, i.e., será $(2a+1)^2 \equiv -3 \pmod{p}$ o sea -3 es un residuo de p. *Q. E. D.*

Además, es evidente que esta demostración (que es independiente de las precedentes) también comprende números primos de la forma $12n + 7$, a los que ya nos referimos en un artículo anterior.

Conviene observar que se podría usar el método de los artículos 109 y 115, pero por brevedad no nos detenemos en estos detalles.

120.

De lo precedente se obtienen fácilmente los siguientes teoremas (ver art. 102, 103 y 105).

I. -3 *es un residuo de todos los números que no pueden dividirse ni por* 8, *ni por* 9, *ni por ningún número primo de la forma* $6n+5$, *y es un no residuo de todos los restantes.*

II. $+3$ *es un residuo de todos los números que no pueden dividirse ni por* 4, *ni por* 9, *ni por ningún primo de la forma* $12n + 5$ *o* $12n + 7$, *y es un no residuo de todos los restantes.*

Se tiene aquí este caso particular:

-3 es un *residuo* de todos los números primos de la forma $3n + 1$, o lo que es lo mismo, *de todos los que son residuos de* 3. Pero es un *no residuo* de todos los números primos de la forma $6n + 5$, o excluido 2, de todos los primos de la forma $3n+2$, *i.e., de todos los primos que son no residuos de* 3. Se ve fácilmente que todos los casos restantes se siguen naturalmente de éste.

Fermat ya conocía las proposiciones sobre los residuos $+3$ y -3, *Opera* de Wallis, T. II, p. 857. Pero el ilustre Euler fue el primero en dar demostraciones, *Comm. nov. Petr.,* T. VIII, p. 105 y siguientes. Esto resulta más admirable puesto que las demostraciones de las proposiciones pertenecientes a los residuos $+2$ y -2 están basadas en artificios bastante parecidos. Véase también el comentario del ilustre Lagrange en *Nouv. Mém. de l' Ac. de Berlin,* 1775, p. 352.

Residuos $+5$ *y* -5.

121.

Por inducción se descubre que $+5$ no es un residuo de ningún número impar de la forma $5n + 2$ o $5n + 3$, i.e., de ningún número impar que sea no residuo de 5. Se demuestra que esta regla no tiene excepción alguna. Sea el número menor que constituya una excepción de esta regla $= t$, éste por lo tanto es un no residuo del

número 5, pero 5 es un residuo de t. Sea $a^2 = 5 + tu$ tal que a sea par y menor que t. Entonces u será impar y menor que t, pero +5 será un residuo de u. Ahora si a no es divisible por 5, tampoco lo será u. Pero es claro que tu es un residuo de 5, por lo que, puesto que t es un no residuo de 5, tampoco lo será u, i.e., existe un no residuo impar del número 5 cuyo residuo es +5, pero menor que t, contrariamente a la hipótesis. Si por otro lado a es divisible por 5, se pone $a = 5b$ y $u = 5v$ de donde $tv \equiv -1 \equiv 4 \pmod 5$, i.e., tv será un residuo del número 5. En lo restante la demostración procede de manera análoga al caso anterior.

122.

Tanto +5 como −5 serán no residuos de todos los números primos que simultáneamente son no residuos de 5 y de la forma $4n+1$, i.e., de todos los números primos de la forma $20n + 13$ o $20n + 17$. Pero +5 será un no residuo y −5 un residuo de todos los números primos de la forma $20n + 3$ o $20n + 7$.

Puede demostrarse de modo parecido que −5 es un no residuo de todos los números primos de las formas $20n + 11$, $20n + 13$, $20n + 17$ y $20n + 19$. Se nota fácilmente de aquí que +5 es un residuo de todos los números primos de la forma $20n+11$ o $20n+19$, pero no residuo de todos los de la forma $20n+13$ o $20n+17$. Puesto que cada número primo, aparte de 2 y 5 (cuyos residuos son ± 5), está contenido en alguna de las formas $20n + 1$, 3, 7, 9, 11, 13, 17, 19, es claro que se puede juzgar ahora a todos, excepto a los que son de la forma $20n + 1$ o de la forma $20n + 9$.

123.

Por inducción se descubre fácilmente que +5 y −5 son residuos de todos los números primos de la forma $20n+1$ o $20n+9$. Ahora bien, si esto es cierto en general, se tendrá una ley elegante, +5 *es un residuo de todos los números primos que sean residuos de* 5 (pues éstos están contenidos en una u otra de las formas $5n+1$ o $5n+4$, o en una de estas otras $20n+1$, 9, 11, 19, de las cuales la tercera y la cuarta ya se han tratado), *pero es un no residuo de todos los números impares que son no residuos de* 5, como ya lo hemos demostrado antes. Ahora es claro que este teorema es suficiente para juzgar si +5 (y también −5 si se considera como producto de +5 y −1) es un residuo o un no residuo de cualquier número dado. Finalmente se observa la analogía de este teorema con aquél que presentamos en el art. 120 sobre el residuo −3.

Pero la verificación de esta inducción no es tan fácil. Cuando se presenta un número primo de la forma $20n + 1$, o más generalmente de la forma $5n + 1$, este asunto puede resolverse de un modo similar al de los artículos 114 y 119. De hecho, sea a un número cualquiera perteneciente al exponente 5 para el módulo $5n + 1$, el cual evidentemente existe por la sección anterior, y se tendrá $a^5 \equiv 1$, o sea $(a-1)(a^4 + a^3 + a^2 + a + 1) \equiv 0 \pmod{5n+1}$. Pero no puede ser $a \equiv 1$, por eso tampoco $a - 1 \equiv 0$; necesariamente será $a^4 + a^3 + a^2 + a + 1 \equiv 0$. Por lo tanto también $4(a^4 + a^3 + a^2 + a + 1) = (2a^2 + a + 2)^2 - 5a^2$ será $\equiv 0$, i.e., $5a^2$ será un residuo de $5n + 1$, de donde también lo será 5, ya que a^2 es un residuo no divisible por $5n + 1$ (pues a no es divisible por $5n + 1$ porque $a^5 \equiv 1$). *Q. E. D.*

Pero el caso donde se presenta un número primo de la forma $5n + 4$ exige artificios más sutiles. Puesto que las proposiciones que necesitamos aquí se tratarán con más generalidad en lo que sigue, aquí lo tocamos brevemente.

I. Si p es un número primo y b un no residuo cuadrático dado de p, el valor de la expresión

$$(A) \ldots \frac{(x + \sqrt{b})^{p+1} - (x - \sqrt{b})^{p+1}}{\sqrt{b}}$$

(se observa con facilidad que el desarrollo de ésta carece de irracionales) siempre será divisible por p, cualquiera que sea el número que se tome para x. De hecho, es claro de la inspección de los coeficientes que se obtienen del desarrollo de A, que todos los términos desde el segundo al penúltimo (inclusive) son divisibles por p y que $A \equiv 2(p+1)(x^p + xb^{\frac{p-1}{2}}) \pmod{p}$. Pero ya que b es un no residuo de p, será $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, (art. 106); pero x^p siempre es $\equiv x$ (sección anterior), de donde $A \equiv 0$. *Q. E. D.*

II. En la congruencia $A \equiv 0 \pmod{p}$ la indeterminada x tiene exponente p y todos los números 0, 1, 2, $\ldots p-1$ serán raíces de ella. Ahora, tómese a e como un divisor de $p + 1$. La expresión

$$\frac{(x + \sqrt{b})^e - (x - \sqrt{b})^e}{\sqrt{b}}$$

(la cual denotamos por B), si se desarrolla, no tendrá irracionales, la indeterminada x tendrá exponente $e - 1$, y resulta de los primeros elementos del análisis que A es divisible (algebraicamente) por B. Ahora digo que existen $e - 1$ valores de x, que sustituidos en B, hacen B divisible por p. En efecto, si $A \equiv BC$, x tendrá exponente $p - e + 1$ en C, y la congruencia $C \equiv 0 \pmod{p}$ tendrá no más que $p - e + 1$ raíces.

De donde resulta evidente que todos los $e-1$ números restantes entre 0, 1, 2, 3, $\ldots p-1$, serán raíces de la congruencia $B \equiv 0$.

III. Ahora supóngase que p es de la forma $5n+4$, $e=5$, b es un no residuo de p, y el número a se determina tal que

$$\frac{(a+\sqrt{b})^5-(a-\sqrt{b})^5}{\sqrt{b}}$$

es divisible por p. Pero esa expresión es

$$= 10a^4+20a^2b+2b^2 = 2((b+5a^2)^2-20a^4)$$

Por lo tanto, también $(b+5a^2)^2-20a^4$ será divisible por p, i.e., $20a^4$ es un residuo de p; pero ya que $4a^4$ es un residuo no divisible por p (de hecho, se comprueba fácilmente que a no puede dividirse por p), también 5 será un residuo de p. *Q. E. D.*

El teorema enunciado en el comienzo de este artículo resulta verdadero.

Notamos que las demostraciones para ambos casos se deben al ilustre Lagrange, *Mém. de l'Ac. de Berlin,* 1775, p. 352 y siguientes.

Sobre ± 7.

124.

Por un método similar se demuestra:

-7 *es un no residuo de cualquier número que sea no residuo de* 7.

Y por inducción se puede concluir:

-7 *es un residuo de cualquier número primo que sea residuo de* 7.

Pero nadie ha demostrado esto rigurosamente hasta ahora. La demostración es fácil para los residuos de 7 cuya forma es $4n-1$; en efecto, por el método conocido del artículo precedente puede mostrarse que $+7$ siempre es un no residuo de tales números primos y así -7 es un residuo. Pero con esto se logra poco, ya que, los casos restantes no pueden tratarse con este método. Sólo podemos resolver un caso de modo similar a los artículos 119 y 123. A saber: si p es un número primo de la forma $7n+1$, y a pertenece al exponente 7 para el módulo p, se observa fácilmente que:

$$\frac{4(a^7-1)}{a-1} = (2a^3+a^2-a-2)^2+7(a^2+a)^2$$

es divisible por p, de donde $-7(a^2+a)^2$ será un residuo de p. Pero $(a^2+a)^2$, como un cuadrado, es un residuo de p y no divisible por p; puesto que se supone que a pertenece al exponente 7, no puede ser ni $\equiv 0$, ni $\equiv -1 \pmod{p}$, i.e., ni a ni $a+1$ serán divisibles por p, ni tampoco lo será el cuadrado $(a+1)^2a^2$. De donde también es evidente que -7 será un residuo de p. Q.E.D.— Pero los números primos de la forma $7n+2$ o $7n+4$ no se prestan a ninguno de los métodos tratados hasta ahora. Esta demostración también fue encontrada primeramente por el ilustre Lagrange en la misma obra.— Posteriormente, en la Sección VII, enseñaremos más generalmente que la expresión $\frac{4(x^p-1)}{x-1}$ siempre puede reducirse a la forma $X^2 \mp pY^2$ (donde hay que tomar el signo superior cuando p es número primo de la forma $4n+1$ y el inferior cuando es de la forma $4n+3$). Aquí X e Y denotan funciones racionales de x, libres de fracciones. El ilustre Lagrange no desarrolló su análisis más allá del caso $p = 7$ (vea p. 352 de su obra).

Preparación para la investigación general.

125.

Puesto que los métodos precedentes no son suficientes para asegurar las demostraciones generales, es momento para exponer otro método libre de este defecto. Iniciamos con un teorema cuya demostración por mucho tiempo nos eludió, aunque a primera vista parezca tan obvio como para que algunos ni siquiera hayan reconocido la necesidad de una demostración. Es éste: *Cualquier número, excepto los cuadrados tomados positivamente, es un no residuo de algunos números primos.* Pero ya que usamos este teorema solamente como una ayuda para demostrar otros, no explicamos más que aquellos casos que necesitaremos para este fin. Los casos restantes se darán más adelante. Demostremos por tanto que *cualquier número primo de la forma* $4n+1$ *tomado positiva o negativamente**) *es un no residuo de algunos números primos,* y, de hecho, (si es > 5) de algunos primos que son menores que sí mismo.

Primero, cuando se presenta un número primo p de la forma $4n+1$ (> 17; aunque $-13N3$ y $-17N5$) tomado *negativamente,* sea $2a$ el primer número par mayor que $\sqrt{p}$; entonces se ve fácilmente que $4a^2$ siempre será $< 2p$ o sea $4a^2 - p < p$. Pero $4a^2 - p$ es de la forma $4n+3$ mientras que $+p$ es un residuo cuadrático de $4a^2 - p$ (ya que $p \equiv 4a^2 \pmod{4a^2-p}$). Por eso si $4a^2 - p$ es un número primo, $-p$ será un no residuo de él; si no, necesariamente algún factor de $4a^2 - p$ será de la forma $4n+3$; como $+p$ también debe ser un residuo de él, $-p$ será un no residuo. *Q. E. D.*

*) Es claro que $+1$ debe ser excluido.

Para un número primo tomado *positivamente* distinguimos dos casos. *Primero* sea p un número primo de la forma $8n+5$; sea a cualquier número positivo $< \sqrt{\frac{1}{2}p}$. Entonces $8n+5-2a^2$ será un número positivo de la forma $8n+5$ u $8n+3$ (según que a sea par o impar) y por lo tanto necesariamente divisible por algún primo de la forma $8n+3$ u $8n+5$, puesto que el producto de cualquier cantidad de números de la forma $8n+1$ y $8n+7$ no puede tener ni la forma $8n+3$ ni $8n+5$. Sea este producto $= q$, así que $8n+5 \equiv 2a^2 \pmod{q}$. Pero 2 será un no residuo de q (art. 112); así también $2a^2$ *) y $8n+5$. *Q. E. D.*

126.

Que cualquier número primo de la forma $8n+1$ tomado positivamente siempre es un no residuo de algún número primo menor que él, no puede demostrarse por artificios tan obvios. Como esta verdad es de gran importancia, no podemos excluir la demostración rigurosa aunque sea algo prolija. Comencemos como sigue:

LEMA: *Si se tienen dos series de números,*

$$A,\ B,\ C,\ \text{etc.}\ldots.(I), \quad A',\ B',\ C',\ \text{etc.}\ldots.(II)$$

(no interesa si el número de términos en un caso es el mismo que en el otro o no) *confeccionadas de manera que, si p denota un número primo cualquiera o la potencia de un número primo, cuando p divide algún término de la segunda serie (o varios), habrá por lo menos tantos términos de la primera serie divisibles por p. Entonces, afirmo que el producto de todos los números* (I) *será divisible por el producto de todos los números* (II).

Ejemplo. Conste (I) de los números 12, 18, 45; (II) de los números 3, 4, 5, 6, 9. Entonces, si tomamos sucesivamente los números 2, 4, 3, 9, 5, encontramos que hay 2, 1, 3, 2, 1 términos en (I) y 2, 1, 3, 1, 1 términos en (II) que son, respectivamente, divisibles por dichos números y el producto de todos los términos $(I) = 9720$ es divisible por el producto de todos los términos (II), 3240.

Demostración. Sea el producto de todos los términos $(I) = Q$, y el producto de todos los términos de la serie $(II) = Q'$. Es evidente que cualquier número primo que es divisor de Q' también será divisor de Q. Ahora mostraremos que cualquier

*) Art. 98. De hecho a^2 es un residuo de q no divisible por q, pues de lo contrario el número primo p también sería divisible por q. Q.E.A.

factor primo de Q' tiene un grado en Q al menos tan alto como lo tiene en Q'. Sea tal divisor p y supongamos que en la serie (I) hay a términos divisibles por p, b términos divisibles por p^2, c términos divisibles por p^3, etc. Las letras a', b', c', etc. denotan lo similar de la serie (II), y se ve fácilmente que p tiene exponente $a+b+c+$ etc. en Q, y $a'+b'+c'+$ etc. en Q'. Pero ciertamente a' no es mayor que a, b' no es mayor que b etc. (por hipótesis); por lo que $a'+b'+c'+$ etc. ciertamente no será $> a+b+c+$ etc.— Puesto que ningún número primo puede tener mayor exponente en Q' que en Q, Q será divisible por Q' (art. 17). *Q. E. D.*

127.

LEMA: *En la progresión* 1, 2, 3, 4, $\ldots n$ *no puede haber más términos divisibles por cualquier número* h, *que en la progresión* a, $a+1$, $a+2$, $\ldots a+n-1$, *que contiene el mismo número de términos.*

En efecto se nota sin dificultad que si n es un múltiplo de h, en ambas progresiones habrá $\frac{n}{h}$ términos que serán divisibles por h; si n no es múltiplo de h, póngase $n = eh + f$, de manera que f sea $< h$. En la primera serie e términos serán divisibles por h, y en la segunda lo serán e o $e+1$ términos.

Como corolario de esto se sigue una proposición conocida de la teoría de los números figurados; a saber, que

$$\frac{a(a+1)(a+2)\cdots(a+n-1)}{1\cdot 2\cdot 3\cdot \ldots n}$$

siempre es un número entero. Pero si no nos equivocamos, nadie lo ha demostrado directamente.

Finalmente, este lema puede expresarse en forma más general:

En la progresión a, $a+1$, $a+2$, $\ldots a+n-1$ existen por lo menos tantos términos congruentes según el módulo h a un número dado cualquiera r como términos divisibles por h haya en 1, 2, 3, $\ldots n$.

128.

TEOREMA. *Sea* a *un número cualquiera de la forma* $8n+1$, p *cualquier número primo a a cuyo residuo es* $+a$, *y finalmente* m *un número arbitrario: entonces yo afirmo que en la progresión*

$$a,\ \frac{1}{2}(a-1),\ 2(a-4),\ \frac{1}{2}(a-9),\ 2(a-16),\ \ldots 2(a-m^2)\ \textit{o}\ \frac{1}{2}(a-m^2)$$

según que m sea par o impar, existen por lo menos tantos términos divisibles por p como existan en la progresión:

$$1,\ 2,\ 3,\ \ldots 2m+1$$

Denotamos por (I) la primera progresión, por (II) la segunda.

Demostración. I. Cuando $p = 2$, en (I) todos los términos aparte del primero, i.e., m términos serán divisibles; habrá igual número también en (II).

II. Sea p un número impar, o el doble de un número impar, o el cuádruplo de un número impar, y $a \equiv r^2 \pmod{p}$. Entonces, en la progresión $-m$, $-(m-1)$, $-(m-2)$, $\ldots +m$ (la que tiene el mismo número de términos que (II) y que denotamos por (III)) por lo menos tantos términos serán congruentes a r, según el módulo p, como términos en (II) sean divisibles por p (artículo precedente). Entre ellos no pueden haber dos iguales en magnitud que difieran en signo*). Cada uno de ellos tendrá un valor correspondiente en la serie (I), el cual será divisible por p. Por supuesto, si $\pm b$ es un término de la serie (III) congruente a r según el módulo p, $a - b^2$ será divisible por p. Por lo tanto, si por un lado b es par, el término de la serie (I), $2(a-b^2)$ será divisible por p. Por otro lado, si b es impar, el término $\frac{1}{2}(a-b^2)$ será divisible por p: pues es evidente que $\frac{a-b^2}{p}$ será entero *par,* dado que $a - b^2$ es divisible por 8, pero p es divisible a lo sumo por 4 (de hecho, por hipótesis a es de la forma $8n+1$ y b^2, por ser el cuadrado de un número impar, es de la misma forma; por lo que la diferencia será de la forma $8n$). De esto finalmente se concluye que tantos términos en la serie (I) son divisibles por p, como en (III) sean congruentes a r según el módulo p, i.e., igual número o más de los que son divisibles por p en (II).

III. Sea p de la forma $8n$ y $a \equiv r^2 \pmod{2p}$. Entonces se observa fácilmente que a, que por hipótesis es un residuo de p, será también un residuo de $2p$. Entonces, en la serie (III) habrá por lo menos tantos términos congruentes a r, según p, como en la (II) sean divisibles por p, y todos ellos serán de magnitudes diferentes. Pero a cada uno de ellos corresponderá algún término divisible por p en (I). En efecto, si $+b$ o $-b \equiv r \pmod{p}$, será $b^2 \equiv r^2 \pmod{2p}$ †), de donde el término $\frac{1}{2}(a-b^2)$ será

*) En efecto, si fuera $r \equiv -f \equiv +f \pmod{p}$, $2f$ sería divisible por p; por lo tanto, también $2a$ (puesto que $f^2 \equiv a \pmod{p}$). Pero esto es posible únicamente cuando $p = 2$, pues por hipótesis a es primo a p. Pero sobre este caso ya hemos hablado por separado.

†) De hecho, $b^2 - r^2 = (b-r)(b+r)$ estará compuesto de dos factores, uno de los cuales es divisible por p (hipótesis) y el otro por 2 (puesto que tanto b como r son impares); de donde $b^2 - r^2$ es divisible por $2p$.

divisible por p. Por lo que en (I) serán divisibles por p por lo menos tantos términos como en (II). *Q. E. D.*

129.

TEOREMA. *Si a es un número primo de la forma $8n+1$, necesariamente habrá algún número primo menor que $2\sqrt{a+1}$ del cual a sea un no residuo.*

Demostración. Sea a un residuo de todos los primos menores que $2\sqrt{a+1}$. Entonces, se observará con facilidad que a también será un residuo de todos los números compuestos menores que $2\sqrt{a+1}$ (refiérase a las reglas por las cuales aprendimos a deducir si un número dado es un residuo de un número compuesto o no: art. 105). Sea m el mayor entero menor que $\sqrt{a}$. Entonces en la serie

$$a,\ \frac{1}{2}(a-1),\ 2(a-4),\ \frac{1}{2}(a-9),\ \ldots 2(a-m^2) \text{ o } \frac{1}{2}(a-m^2) \qquad (I)$$

serán divisibles por algún número menor que $2\sqrt{a}+1$ tantos o más términos como en ésta:

$$1,\ 2,\ 3,\ 4,\ \ldots 2m+1 \quad \text{(art. precedente)} \qquad (II)$$

De esto se sigue que el producto de todos los términos en (I) es divisible por el producto de todos los términos en (II) (art. 126). Pero esto o es $= a(a-1)(a-4)\cdots(a-m^2)$ o bien la mitad de este producto (según que m sea par o impar). Por lo que el producto $a(a-1)(a-4)\cdots(a-m^2)$ puede dividirse por el producto de todos los términos en (II), y, puesto que todos estos términos son primos a a, también lo será su producto, omitido el factor a. Pero el producto de todos los términos de (II) también puede presentarse así:

$$(m+1)\cdot((m+1)^2-1)\cdot((m+1)^2-4)\cdot\cdots\cdot((m+1)^2-m^2)$$

Por lo tanto

$$\frac{1}{m+1}\cdot\frac{a-1}{(m+1)^2-1}\cdot\frac{a-4}{(m+1)^2-4}\cdot\cdots\cdot\frac{a-m^2}{(m+1)^2-m^2}$$

será un número entero, aunque sea un producto de fracciones menores que la unidad: puesto que en efecto $\sqrt{a}$ necesariamente debe ser irracional, será $m+1>\sqrt{a}$. Y por lo tanto $(m+1)^2>a$. De esto finalmente se concluye que nuestra suposición no puede tener lugar. *Q. E. D.*

Ahora, puesto que ciertamente $a>9$, tendremos $2\sqrt{a}+1<a$. Por lo tanto existirá algún primo $<a$ del cual a es un no residuo.

Por inducción se apoya un teorema general (fundamental), y se deducen algunas conclusiones de él.

130.

Después de haber demostrado rigurosamente que cada número primo de la forma $4n + 1$, tomado positivo o negativamente, es un no residuo de algún número primo menor que él mismo, pasamos entonces a una comparación más exacta y más general de los números primos, para ver cuando uno es un residuo o un no residuo del otro.

Con todo rigor, hemos demostrado arriba que -3 y $+5$ son residuos o no residuos de todos los números primos que son residuos o no residuos respectivamente de 3 y 5.

Se encuentra por inducción que los números -7, -11, $+13$, $+17$, -19, -23, $+29$, -31, $+37$, $+41$, -43, -47, $+53$, -59, etc., son residuos o no residuos de todos los números primos, los cuales tomados positivamente, resultan residuos o no residuos de estos primos respectivamente. Esta inducción puede llevarse a cabo fácilmente con ayuda de la tabla II.

Quienquiera, con un poco de atención, notará que de estos números primos aquéllos con signo positivo son los de la forma $4n + 1$, y los de signo negativo son los de la forma $4n + 3$.

131.

Demostraremos en seguida que lo que descubrimos por inducción tiene lugar en general. Pero, antes de entrar en este trabajo, será necesario extraer todo lo que sigue de este teorema, si se supone verdadero. Enunciamos el teorema mismo así:

Si p es un número primo de la forma $4n + 1$, $+p$ será un residuo o no residuo de cualquier número primo que, tomado positivamente, es un residuo o no residuo del mismo p. Si p es un número primo de la forma $4n + 3$, $-p$ tendrá la misma propiedad.

Ya que casi todo lo que puede decirse sobre los residuos cuadráticos se apoya en este teorema, la denominación *teorema fundamental* que usaremos en lo que sigue no será inconveniente.

Para poder presentar nuestro razonamiento lo más brevemente posible, denotaremos por a, a', a'', etc. los números primos de la forma $4n + 1$, por b, b', b'', etc. los números primos de la forma $4n + 3$; por A, A', A'', etc. los números cualesquiera de la forma $4n + 1$, por B, B', B'', etc. los números cualesquiera de

la forma $4n+3$. Finalmente la letra R puesta entre dos cantidades indicará que la primera es un residuo de la siguiente, mientras que la letra N tendrá el significado contrario. Por ejemplo, $+5R11$, $\pm 2N5$ indicará que $+5$ es un residuo de 11, pero $+2$ y -2 son no residuos de 5. Ahora, al unir el teorema fundamental con los teoremas del art. 111 fácilmente se deducirán las siguientes proposiciones.

	Si		será
1.	$\pm aRa'$	.....	$\pm a'Ra$
2.	$\pm aNa'$	.....	$\pm a'Na$
3.	$\left\{\begin{matrix}+aRb\\-aNb\end{matrix}\right\}$	.....	$\pm bRa$
4.	$\left\{\begin{matrix}+aNb\\-aRb\end{matrix}\right\}$	.....	$\pm bNa$
5.	$\pm bRa$	.....	$\left\{\begin{matrix}+aRb\\-aNb\end{matrix}\right.$
6.	$\pm bNa$	.....	$\left\{\begin{matrix}+aNb\\-aRb\end{matrix}\right.$
7.	$\left\{\begin{matrix}+bRb'\\-bNb'\end{matrix}\right\}$	.....	$\left\{\begin{matrix}+b'Nb\\-b'Rb\end{matrix}\right.$
8.	$\left\{\begin{matrix}+bNb'\\-bRb'\end{matrix}\right\}$	.....	$\left\{\begin{matrix}+b'Rb\\-b'Nb\end{matrix}\right.$

132.

En esta tabla están contenidos todos los casos que pueden ocurrir al comparar dos números primos: lo que sigue corresponderá a números cualesquiera, pero sus demostraciones son menos obvias.

	Si		será
9.	$\pm aRA$	.....	$\pm ARa$
10.	$\pm bRA$	.....	$\left\{\begin{matrix}+ARb\\-ANb\end{matrix}\right.$
11.	$+aRB$	.....	$\pm BRa$
12.	$-aRB$	.....	$\pm BNa$
13.	$+bRB$	.....	$\left\{\begin{matrix}-BRb\\+BNb\end{matrix}\right.$
14.	$-bRB$	.....	$\left\{\begin{matrix}+BRb\\-BNb\end{matrix}\right.$

Puesto que los mismos principios conducen a las demostraciones de todas estas proposiciones, no será necesario desarrollarlas todas: la demostración de la proposición 9 que adjuntamos puede servir como ejemplo. Ante todo se notará que cada número de la forma $4n + 1$ puede tener o ningún factor de la forma $4n + 3$, o dos, o cuatro, etc., i.e., el número de tales factores (entre los cuales varios pueden ser iguales) siempre será un número par. Por otro lado, cualquier número de la forma $4n + 3$ tendrá un número impar de factores de la forma $4n + 3$ (i.e., o uno, o tres, o cinco etc.). El número de factores de la forma $4n + 1$ permanece indeterminado.

La *Proposición 9* se demuestra de la siguiente forma. Sea A el producto de los factores primos a', a'', a''', etc., b, b', b'', etc.; donde el número de factores b, b', b'', etc. es par (puede también que no haya ninguno, lo que se reduce a lo mismo). Ahora, si a es un residuo de A, también será un residuo de todos los factores a', a'', a''', etc., b, b', b'', etc.; de donde por las proposiciones 1 y 3 del artículo precedente cada uno de estos factores serán residuos de a; por lo tanto también el producto A, lo mismo que $-A$; sin embargo, si $-a$ es un residuo de A y por lo tanto de los factores a', a'', etc., b, b', etc., cada uno de a', a'', etc. será un residuo de a, y cada uno de b, b', etc. un no residuo. Pero como el número de estos últimos es par, el producto de todos, esto es A, será un residuo de a, y así también lo será $-A$.

133.

Iniciamos ahora una investigación más general. Consideraremos dos números impares cualesquiera P y Q, primos entre sí, provistos de signos cualesquiera. Concíbase a P resuelto en sus factores primos sin consideración de su signo, y se denotará por p el número de estos factores para los cuales Q sea un no residuo. Si algún número primo, del cual Q es un no residuo, aparece varias veces entre los factores de P, también deberán ser contados varias veces. De modo semejante, sea q el número de factores primos de Q de los cuales P es un no residuo. Entonces los número p y q tendrán cierta relación dependiente de la naturaleza de los números P y Q. En efecto, si uno de los números p o q es par o impar la forma de los números P y Q mostrará si el otro es par o impar. Se presentará esta relación en la siguiente tabla.

Los números p y q serán al mismo tiempo pares o al mismo tiempo impares,

cuando los números P y Q tienen las formas:

1.	$+A,$	$+A'$
2.	$+A,$	$-A'$
3.	$+A,$	$+B$
4.	$+A,$	$-B$
5.	$-A,$	$-A'$
6.	$+B,$	$-B'$

En el caso contrario, uno de los números p o q será par, y el otro impar, cuando los números P y Q tienen las formas:

7.	$-A,$	$+B$
8.	$-A,$	$-B$
9.	$+B,$	$+B'$
10.	$-B,$	$-B'$*)

Ejemplo. Dados los números -55 y $+1197$, que representan el cuarto caso, entonces 1197 es un no residuo de un solo factor primo de 55, en efecto, del número 5, mientras que -55 es un no residuo de tres factores primos de 1197, a saber, de los números 3, 3 y 19.

Si P y Q denotan números primos, estas proposiciones se convierten en las que hemos tratado en el art. 131. De hecho, aquí p y q no pueden ser mayores que 1; por lo que cuando p se toma par, necesariamente será $= 0$, i.e., Q será un residuo de P, pero cuando p es impar, Q será un no residuo de P, y vice-versa. Así, si se escribe a y b en lugar de A y B, se sigue de 8 que si $-a$ es un residuo o no residuo de b, $-b$ será un no residuo o residuo de a, lo que coincide con 3 y 4 del art. 131.

Por lo general es evidente que Q no puede ser un no residuo de P a no ser que $p = 0$. Por lo tanto, si p es impar, ciertamente Q será un no residuo de P.

De aquí también pueden derivarse sin dificultad las proposiciones del artículo precedente.

Por otra parte, pronto será evidente que esta representación general es más que una observación estéril, puesto que la demostración completa del teorema fundamental apenas podría completarse sin ella.

*) Sea $l = 1$ si ambos P, $Q \equiv 3 \pmod 4$; si no, sea $l = 0$, y sea $m = 1$ si ambos P y Q son negativos, y $m = 0$ en el caso contrario. Así la relación depende de $l + m$.

134.

Ahora nos dirigimos a deducir estas proposiciones.

I. Como antes, tómese P resuelto en sus factores primos sin tomar en consideración los signos y Q resuelto en factores de cualquier modo pero donde, no obstante, se considera el signo de Q. Se combina cada uno de aquellos factores con cada uno de éstos. Si s denota el número de todas las combinaciones en las cuales el factor de Q es un no residuo del factor de P, entonces p y s serán al mismo tiempo pares o impares. De hecho, sean f, f', f'', etc. los factores primos de P, y entre los factores en los que está resuelto Q, sea m el número que son no residuos de f, m' el de los no residuos de f', m'' el de los no residuos de f'', etc. Entonces se verá fácilmente que

$$s = m + m' + m'' + \text{ etc.}$$

y que p expresa cuántos números entre m, m', m'', etc. son impares. De donde es evidente que s será par cuando p sea par, pero impar cuando p sea impar.

II. Esto vale generalmente para cualquier forma en que Q sea resuelto en factores. Pasemos a los casos particulares. Consideraremos primero el caso donde uno de los números P es positivo, pero el otro, Q, es o bien de la forma $+A$ o bien de la forma $-B$. Se resuelven P y Q en sus factores primos, donde se les da un signo positivo a cada uno de los factores de P, pero a los factores individuales de Q el signo positivo o el negativo según sean de la forma a o b. Entonces, como se requiere, es evidente que Q será de la forma $+A$ o $-B$. Se combinan cada uno de los factores de P con cada uno de los de Q y se denotará como antes por s el número de combinaciones en que cada factor de Q es un no residuo del factor de P, y de modo semejante por t el número de combinaciones en que cada factor de P es un no residuo del factor de Q. Se sigue del teorema fundamental que estas combinaciones serán idénticas, de donde $s = t$. Finalmente de lo que hemos demostrado se sigue que $p \equiv s \pmod 2$, $q \equiv t \pmod 2$, y así $p \equiv q \pmod 2$.

Así pues se tienen las proposiciones 1, 3, 4 y 6 del art. 133.

Las restantes proposiciones pueden derivarse directamente por métodos similares, pero requieren de una nueva consideración. Sin embargo, se derivan más fácilmente de lo anterior por los métodos siguientes.

III. De nuevo P y Q denotan números impares cualesquiera, primos entre sí, p y q el número de factores primos de P y Q de los que Q y P son no residuos respectivamente. Finalmente sea p' el número de factores primos de P de los cuales

$-Q$ es un no residuo (cuando Q es negativo es evidente que $-Q$ indicará un número positivo). Ahora se distribuyen todos los factores primos de P en cuatro clases.

1) Factores de la forma a, de los cuales Q es un residuo.

2) Factores de la forma b, de los cuales Q es un residuo. Sea χ el número de ellos.

3) Factores de la forma a, de los cuales Q es un no residuo. Sea ψ el número de ellos.

4) Factores de la forma b, de los cuales Q es un no residuo. Sea ω el número de ellos.

Entonces se ve fácilmente que $p = \psi + \omega$, $p' = \chi + \psi$.

Cuando P es de la forma $\pm A$, $\chi + \omega$ y también $\chi - \omega$, serán números pares: por lo que $p' = p + \chi - \omega \equiv p \pmod 2$. Pero cuando P es de la forma $\pm B$, se descubre por un razonamiento similar que los números p y p' serán incongruentes, según mod. 2.

IV. Apliquemos esto a cada uno de los casos. Primero, sean tanto P como Q de la forma $+A$, entonces de la proposición 1 tendremos $p \equiv q \pmod 2$; pero $p' \equiv p \pmod 2$; por lo que también $p' \equiv q \pmod 2$. Lo cual concuerda con la proposición 2.— De modo semejante si P es de la forma $-A$, Q de la forma $+A$, será $p \equiv q \pmod 2$ de la proposición 2 la que ya hemos demostrado. De esto si $p' \equiv p$ tendremos $p' \equiv q$. Así pues, también la proposición 5 está demostrada.

De la misma manera se deriva la proposición 7 de la 3, la proposición 8 o de la 4 o de la 7; la 9 de la 6; la 10 de la 6.

Demostración rigurosa del teorema fundamental.

135.

Las proposiciones del artículo 133 no se han demostrado por medio del artículo precedente, sino que se mostró que la validez de ellas depende de la validez del teorema fundamental que hemos supuesto. Por el método de esta misma deducción es evidente que estas proposiciones valdrán para números P y Q si el teorema fundamental vale para todos los factores primos de estos números comparados entre sí, y aún si no fuera válido en general. Por lo tanto ahora avanzamos hacia la demostración del teorema fundamental. Enunciamos antes de ella la siguiente aclaración.

Diremos que el teorema fundamental es verdadero hasta algún número M, si vale para dos números primos cualesquiera de los cuales ninguno supera a M.

De modo semejante debe entenderse si decimos que los teoremas de los artículos 131, 132 y 133 son verdaderos hasta algún término. Se nota fácilmente que si el teorema fundamental es válido hasta algún término, estas proposiciones tendrán que ser válidas hasta el mismo término.

136.

Por inducción puede confirmarse fácilmente que el teorema fundamental vale para números pequeños, de tal manera se determina un límite hasta el cual sea válido. Suponemos que esta inducción está hecha; es completamente indiferente hasta donde la hayamos realizado. De tal manera bastaría confirmarlo hasta al número 5, pero esto se logra con la simple observación de que $+5N3$, $\pm 3N5$.

Ahora, si el teorema fundamental no es verdadero en general, existirá algún límite T hasta el cual valdrá, de manera que ya no valga más para el próximo número mayor $T+1$. Esto es lo mismo que si dijéramos que existen dos números primos, de los cuales el mayor es $T+1$ y que comparados entre sí contradicen el teorema fundamental, y dijéramos que otros pares cualesquiera de números primos, siendo ambos menores que $T+1$, cumplen con este teorema. De donde se sigue que las proposiciones de los artículos 131, 132, 133 también deberán ser válidas hasta T. Pero mostraremos ahora que esta suposición no puede subsistir. Los casos siguientes deberán distinguirse según las formas diferentes que pueden tener, tanto $T+1$ como el número primo menor que $T+1$ que contradiría el teorema. Denotemos este número primo por p.

Cuando tanto $T+1$ como p son de la forma $4n+1$, el teorema fundamental puede ser falso de dos maneras, a saber, si al mismo tiempo fuera

o bien $\pm pR(T+1)$ y $\pm(T+1)Np$

o bien a la vez $\pm pN(T+1)$ y $\pm(T+1)Rp$

Cuando tanto $T+1$ como p son de la forma $4n+3$, el teorema fundamental sería falso si al mismo tiempo tuvieramos

o bien $+pR(T+1)$ y $-(T+1)Np$

(o lo que es lo mismo $-pN(T+1)$ y $+(T+1)Rp$)

o bien $+pN(T+1)$ y $-(T+1)Rp$

(o sea $-pR(T+1)$ y $+(T+1)Np$)

Cuando $T+1$ es de la forma $4n+1$, y p es de la forma $4n+3$, el teorema fundamental sería falso si tuvieramos

o bien $\pm pR(T+1)$ y $+(T+1)Np$ (o $-(T+1)Rp$)

o bien $\pm pN(T+1)$ y $-(T+1)Np$ (o $+(T+1)Rp$)

Cuando $T+1$ es de la forma $4n+3$ y p de la forma $4n+1$, el teorema fundamental sería falso si tuvieramos

o bien $+pR(T+1)$ (o $-pN(T+1)$) y $\pm(T+1)Np$
o bien $+pN(T+1)$ (o $-pR(T+1)$) y $\pm(T+1)Rp$

Si se puede demostrar que ninguno de estos ocho casos puede tener lugar, sería cierto al mismo tiempo que la validez del teorema fundamental no está acotada por ningún límite. Ahora pasamos a este asunto, pero, puesto que algunos de estos casos son dependientes de otros, no convendrá mantener el mismo orden que hemos usado aquí para enumerarlos.

137.

Primer caso. Cuando $T+1$ es de la forma $4n+1$ $(=a)$, y p es de la misma forma, si $\pm pRa$, entonces no puede ser que $\pm aNp$. Esto era el primer caso arriba.

Sea $+p \equiv e^2 \pmod{a}$, donde e es par y $< a$ (esto siempre es posible). Ahora deben distinguirse dos casos.

I. Cuando e no es divisible por p, se pone $e^2 = p + af$ y f será positivo de la forma $4n+3$ (o sea de la forma B), $< a$, y no divisible por p. Además tendremos $e^2 \equiv p \pmod{f}$, i.e., pRf de donde por la proposición 11 del art. 132 $\pm fRp$ (en efecto $p, f < a$, y para ellos, estas proposiciones valdrán). Pero también $afRp$, por lo tanto $\pm aRp$.

II. Cuando e es divisible por p, se pone $e = gp$ y así $e^2 = p + aph$ o sea $pg^2 = 1 + ah$. Entonces, h será de la forma $4n+3$ (B), y primo a g^2 y p. Además, tendremos pg^2Rh pues también pRh, y de esto (proposición 11, art. 132) $\pm hRp$. Y también $-ahRp$, porque $-ah \equiv 1 \pmod{p}$; por lo tanto también será $\mp aRp$.

138.

Segundo caso. Cuando $T+1$ es de la forma $4n+1$ $(=a)$, p de la forma $4n+3$, y $\pm pR(T+1)$, no puede ser ni $+(T+1)Np$ ni $-(T+1)Rp$. Este caso fue el quinto arriba.

Sea como antes $e^2 = p + fa$, donde e es par y $< a$.

I. Cuando e no es divisible por p, tampoco f será divisible por p. Además de esto f será positivo de la forma $4n+1$ (o sea A), y $< a$, pero $+pRf$; por lo tanto (proposición 10 del art. 132) $+fRp$. Pero también $+faRp$, de donde tendremos $+aRp$, o $-aNp$.

II. Cuando e es divisible por p, sea $e = pg$ y $f = ph$. Así que tendremos $g^2p = 1 + ha$. Entonces h será positivo de la forma $4n+3$ (B), y primo a p y g^2. Además $+g^2pRh$, así que $+pRh$; de esto (proposición 13, art. 132) $-hRp$. Pero $-haRp$, de donde $+aRp$ y $-aNp$.

139.

Tercer caso. Cuando $T+1$ es de la forma $4n+1$ ($= a$), p de la misma forma y $\pm pNa$, entonces no puede ser que $\pm aRp$. (Segundo caso arriba).

Tomemos algún número primo menor que a, del cual $+a$ sea un no residuo, el cual, hemos demostrado arriba, existe. Conviene considerar aquí dos casos por separado, según que este número primo sea de la forma $4n+1$ o $4n+3$; pues no se ha demostrado que existan tales números primos de *ambas* formas.

I. Sea ese número primo $= a'$ y de la forma $4n+1$. Entonces tendremos $\pm a'Na$ (art. 131) ya que $\pm a'pRa$. Sea por lo tanto $e^2 \equiv a'p \pmod{a}$ y e par, $< a$. Entonces deberán distinguirse cuatro casos.

1) Cuando e no es divisible ni por p ni por a'; ponemos $e^2 = a'p \pm af$ tomado el signo de tal manera que f sea positivo. Entonces será $f < a$, primo a a' y a p y para el signo superior, de la forma $4n+3$, para el inferior de la forma $4n+1$. Por brevedad denotaremos por $[x, y]$ el número de factores primos del número y de los cuales x es un no residuo. Entonces será $a'pRf$ y así $[a'p, f] = 0$. De esto $[f, a'p]$ será un número par (las proposiciones 1 y 3 del art. 133), i.e., o bien $= 0$, o bien $= 2$. Por lo que f será o bien un residuo de ambos números a' y p o bien de ninguno. Pero lo primero es imposible ya que $\pm af$ es un residuo de a' y $\pm aNa'$ (hipótesis); de donde $\pm fNa'$. De esto f tiene que ser un no residuo de ambos números a' y p. Pero puesto que $\pm afRp$, tendremos $\pm aNp$. *Q. E. D.*

2) Cuando e es divisible por p pero no por a', sea $e = gp$ y $g^2p = a' \pm ah$, el signo determinado tal que h sea positivo. Entonces tendremos $h < a$, primo a a', g y p, para el signo superior de la forma $4n+3$, pero para el inferior de la forma $4n+1$. De la ecuación $g^2p = a' \pm ah$, si se la multiplica por p y a', puede deducirse

sin dificultad alguna que

$$pa'Rh \ldots\ldots (\alpha)$$
$$\pm ahpRa' \ldots\ldots (\beta)$$
$$aa'hRp \ldots\ldots (\gamma)$$

Sigue de (α) que $[pa', h] = 0$, por lo que (proposiciones 1 y 3, art. 133) $[h, pa']$ es par, i.e., h será un no residuo o de ambos p y a', o de ninguno. *En el primer caso,* sigue de (β) que $\pm apNa'$, y ya que por hipótesis $\pm aNa'$, será $\pm pRa'$. De esto, por el teorema fundamental que vale para los números p y a', puesto que son menores que $T+1$, tendremos $\pm a'Rp$. Ya que hNp, entonces por (γ), $\pm aNp$. *Q. E. D. En el segundo caso,* sigue de (β) que $\pm apRa'$, de esto $\pm pNa'$, $\pm a'Np$, y finalmente de esto y de hRp se tiene de (γ) que $\pm aNp$. *Q. E. D.*

3) Cuando e es divisible por a' pero no por p. Para este caso la demostración procede de un modo semejante al precedente y no es necesario detenerse en ésta.

4) Cuando e es divisible tanto por a' como por p, y por tanto también por el producto $a'p$ (hemos supuesto que los números a' y p son *diferentes,* puesto que en el caso contrario, aNp estará contenido en la hipótesis aNa'). Sea $e = ga'p$ y $g^2a'p = 1 \pm ah$. Entonces tendremos $h < a$, primo a a' y p, para el signo superior de la forma $4n+3$, y para el inferior de la forma $4n+1$. Pero se observa fácilmente que de esta ecuación pueden deducirse las siguientes:

$$a'pRh \ldots\ldots (\alpha)$$
$$\pm ahRa' \ldots\ldots (\beta)$$
$$\pm ahRp \ldots\ldots (\gamma)$$

De (α), que coincide con (α) en 2), se sigue igualmente como allí. Esto es, al mismo tiempo se tiene o bien hRp, hRa', o bien hNp, hNa'. Pero en el primer caso, por (β) será aRa', contrariamente a la hipótesis; por lo cual será hNp, y así también por (γ), aNp.

II. Cuando ese número primo es de la forma $4n+3$, la demostración es tan similar a la precedente que no es importante adjuntarla. Para quienes desean desarrollarla (lo que recomendamos bastante), notamos que después de haber llegado a la ecuación $e^2 = bp \pm af$ (denotando a b como aquel número primo) será útil si se consideran por separado ambos signos.

140.

Cuarto caso. Cuando $T+1$ es de la forma $4n+1$ $(=a)$, p de la forma $4n+3$, y $\pm pNa$, no podrán ser ni $+aRp$ ni $-aNp$. (El sexto caso arriba).

También por brevedad omitimos la demostración de este caso, puesto que es completamente similar a la demostración del tercer caso.

141.

Quinto caso. Cuando $T+1$ es de la forma $4n+3$ $(=b)$, p de la misma forma, y $+pRb$ o $-pNb$, no será ni $+bRp$ ni $-bNp$. (Tercer caso arriba).

Sea $p \equiv e^2 \pmod{b}$, y e par y $< b$.

I. Cuando e no es divisible por p. Póngase $e^2 = p+bf$ y f será positivo, de la forma $4n+3$, $< b$ y primo a p. Además tendremos pRf, por tanto por la proposición 13, art. 132, $-fRp$. De esto y de $+bfRp$ tenemos $-bRp$ y así $+bNp$. *Q. E. D.*

II. Cuando e es divisible por p, sea $e = pg$ y $g^2p = 1 + bh$. Entonces tendremos h de la forma $4n+1$ y primo a p, $p \equiv g^2p^2 \pmod{h}$, por tanto pRh. De esto es $+hRp$ (proposición 10, art. 132), y de $-bhRp$ se sigue que $-bRp$ o sea $+bNp$. *Q. E. D.*

142.

Sexto caso. Cuando $T+1$ es de la forma $4n+3$ $(=b)$, p de la forma $4n+1$, y pRb, no puede ser $\pm bNp$. (El séptimo caso arriba.)

Omitimos la demostración, que es totalmente semejante a la precedente.

143.

Séptimo caso. Cuando $T+1$ es de la forma $4n+3$ $(=b)$, p de la misma forma, y $+pNb$ o $-pRb$, no pueden ser $+bNp$, ni $-bRp$. (Cuarto caso arriba).

Sea $-p \equiv e^2 \pmod{b}$, y e par y $< b$.

I. Cuando e no es divisible por p. Sea $-p = e^2 - bf$, y f será positivo, de la forma $4n+1$, primo a p y menor que b (ya que ciertamente e no es mayor que $b-1$, $p < b-1$, por lo que tendremos $bf = e^2 + p < b^2 - b$ i.e., $f < b-1$). Además tendremos $-pRf$, de esto (proposición 10, art. 132) $+fRp$, de $+bfRp$ tendremos $+bRp$, o $-bNp$.

II. Cuando e es divisible por p, sea $e = pg$, y $g^2p = -1 + bh$. Entonces será h positivo, de la forma $4n+3$, primo a p y $< b$. Además tendremos $-pRh$, de donde (proposición 14, art. 132) $+hRp$. De $bhRp$ sigue que $+bRp$ o $-bNp$. *Q. E. D.*

144.

Octavo caso. Cuando $T+1$ *es de la forma* $4n+3$ *(*$= b$*),* p *de la forma* $4n+1$*,* y $+pNb$ *o* $-pRb$*, no puede ser* $\pm bRp$*.* (El último caso arriba).

La demostración es como en el caso precedente.

Método análogo para la demostración del teorema del art. 114.

145.

En la demostración precedente siempre tomamos para e un valor par (art. 137–144). Conviene observar también que pudimos usar un valor impar, pero entonces hubiéramos tenido que introducir para esto más distinciones. Quienes se deleitan con estas investigaciones las encontrarán útiles si ponen esfuerzo en el desarrollo de estos casos. Además, los teoremas pertenecientes a los residuos $+2$ y -2 entonces deberían suponerse; pero como nuestra demostración está completa sin usar estos teoremas, obtenemos de esto un método nuevo para demostrarlos. Este no se debe desdeñar, ya que es más directo que los métodos que utilizamos arriba para demostrar que ± 2 es un residuo de cualquier número primo de la forma $8n+1$. Supondremos que los casos restantes (que abarcan los números primos de las formas $8n+3$, $8n+5$, $8n+7$) ya han sido demostrados mediante los métodos tratados arriba, y que este teorema solamente ha sido establecido por inducción. No obstante, llevaremos esta inducción a un nivel de certidumbre mediante las siguientes reflexiones.

Si ± 2 no es un residuo de todos los números primos de la forma $8n+1$, póngase el menor primo de esta forma del cual ± 2 es un no residuo $= a$, así que el teorema vale para todos los primos menores que a. Entonces, se toma algún número primo $< \frac{1}{2}a$, del cual a es un no residuo (del articulo 129 se deduce con facilidad que tal número existe). Sea este número $= p$, por el teorema fundamental resultará pNa. De esto, $\pm 2pRa$.— Por eso, sea $e^2 \equiv 2p \pmod{a}$, de manera que e sea impar y $< a$. Entonces deberán distinguirse dos casos.

I. Cuando e no es divisible por p. Sea $e^2 = 2p + aq$, así que q será positivo, de la forma $8n+7$ o de la forma $8n+3$ (según que p sea de la forma $4n+1$ o $4n+3$), $< a$, y no divisible por p. Todos los factores primos de q se distribuirán en

cuatro clases, a saber: sean e aquéllos de la forma $8n+1$, f de la forma $8n+3$, g de la forma $8n+5$, h de la forma $8n+7$. Sea E el producto de los factores de la primera clase y los productos de los factores de la segunda, tercera, y cuarta clases respectivamente F, G, H*). Hecho esto, consideraremos *primero* el caso donde p es de la forma $4n+1$ y q de la forma $8n+7$. Entonces se ve fácilmente que $2RE$ y $2RH$, de donde pRE y pRH y de esto finalmente ERp y HRp. Además 2 será un no residuo de cualquier factor de la forma $8n+3$ u $8n+5$, y por eso también p; y este factor será un no residuo de p; de donde se concluye fácilmente que FG será un residuo de p si $f+g$ es par, no residuo si $f+g$ es impar. Pero $f+g$ no puede ser impar; de hecho, enumerando todos los casos se nota fácilmente que $EFGH$ o sea q será de la forma $8n+3$ u $8n+5$ si $f+g$ es impar, sean como sean e, f, g, h por separado, contrariamente a la hipótesis. Por lo tanto, tendremos $FGRp$, $EFGHRp$, o sea qRp, y finalmente $aqRp$ implica aRp, contrariamente a la hipótesis. *Segundo*, cuando p es de la forma $4n+3$, puede demostrarse de modo semejante que será pRE, así que ERp y $-pRF$, y en consecuencia FRp, finalmente $g+h$ es par y así $GHRp$, de donde finalmente se sigue que qRp y aRp, contrariamente a la hipótesis.

II. Cuando e es divisible por p, la demostración puede prepararse de modo semejante y puede ser desarrollada sin dificultad por los expertos (para quienes se escribió este artículo). Por brevedad la omitimos.

La resolución del problema general.

146.

Por el teorema fundamental y las proposiciones pertenecientes a los residuos -1 y ± 2, siempre puede determinarse si un número dado cualquiera es un residuo o un no residuo de un número primo dado. Pero será útil presentar de una manera clara lo que hemos dicho arriba para que se tenga reunido todo lo necesario para la resolución.

PROBLEMA. *Propuestos dos números cualesquiera P y Q, descubrir si uno de ellos Q es un residuo o no residuo del otro P.*

Resolución. I. Sea $P = a^\alpha b^\beta c^\gamma$ etc. donde a, b, c, etc. denotan números primos diferentes positivos (puesto que se toma el valor absoluto de P). Por brevedad, en este artículo hablaremos simplemente de una *relación* de dos números x e y si el

*) Si no hubiera factores de una clase, debería escribirse 1 en vez del producto de ellos.

primero x es un residuo o no residuo de y. Por tanto, la relación de Q y P depende de las relaciones de Q y a^α; Q y b^β etc. (art. 105).

II. Para saber la relación de Q y a^α (y de los restantes Q y b^β etc.) deben distinguirse dos casos.

1. Cuando Q es divisible por a. Póngase $Q = Q'a^e$ de manera que Q' no sea divisible por a. Entonces si $e = \alpha$ o $e > \alpha$ tendremos QRa^α, pero si $e < \alpha$ e impar tendremos QNa^α: finalmente si $e < \alpha$ y par, Q tendrá con a^α la misma relación que tiene Q' con $a^{\alpha-e}$. Así este caso se reduce al caso:

2. Cuando Q no es divisible por a. Aquí de nuevo distinguimos dos casos.

(A) Cuando $a = 2$. Entonces siempre tendremos QRa^α cuando $\alpha = 1$; pero cuando $\alpha = 2$, se requiere que Q sea de la forma $4n + 1$. Finalmente, cuando $\alpha = 3$ o > 3, Q debe ser de la forma $8n + 1$. Si se cumple esta condición tendremos QRa^α.

(B) Cuando a es algún otro número primo. Entonces Q tendrá con a^α la misma relación que tiene con a. (Véase art. 101).

III. Investíguese la relación de un número cualquiera Q con un número primo (impar) a de la manera siguiente. Cuando $Q > a$, sustitúyase en lugar de Q el menor residuo positivo de él según el módulo a*). Este tendrá la misma relación con Q que tiene a.

Ahora resuélvase Q, o el número tomado en su lugar, en sus factores primos p, p', p'', etc., adjuntando el factor -1 cuando Q es negativo. Entonces resulta que la relación de Q con a depende de las relaciones de cada uno de p, p', p'', etc. con a. A saber, si entre aquellos factores, $2m$ son no residuos de a, resultará QRa, pero si son $2m + 1$ factores, tendremos QNa. Se nota fácilmente que si entre los factores p, p', p'', etc. dos o cuatro o seis de ellos o en general $2k$ resultan iguales, ellos pueden con seguridad eliminarse.

IV. Si entre los factores p, p', p'' se encuentran -1 y 2, la relación de éstos con a puede encontrarse en los artículos 108, 112, 113, 114. La relación de los restantes con a depende de las relaciones de a con ellos (teorema fundamental y proposiciones del art. 131). Sea p uno de ellos, y se encontrará (tratando los números a y p del mismo modo como antes se trataron Q y a, que eran respectivamente mayores) que la relación de a con p o puede determinarse mediante los artículos 108–114 (si en efecto el menor residuo de a (mod. p) no tiene ningún factor primo impar), o depende de la relación de p con ciertos números primos menores que p. Lo mismo vale para los restantes factores p', p'', etc. Ahora se ve fácilmente que continuando con esta

*) Residuo en el sentido del art. 4. En general conviene tomar el menor residuo *absoluto.*

operación finalmente se llega a números cuyas relaciones pueden determinarse por las proposiciones de los art. 108–114. Con un ejemplo será más claro.

Ejemplo. Se quiere la relación del número $+453$ con 1236. Tenemos $1236 = 4 \cdot 3 \cdot 103$; $+453R4$ por II.2(A); $+453R3$ por II.1. Por lo tanto queda examinar la relación de $+453$ con 103. Ella será la misma que tendrá $+41$ ($\equiv 453 \pmod{103}$) con 103; la misma que $+103$ con 41 (teorema fundamental) o sea de -20 con 41. Pero $-20R41$; puesto que $-20 = -1 \cdot 2 \cdot 2 \cdot 5$; $-1R41$ (art. 108); y $+5R41$ porque $41 \equiv 1$ y es un residuo de 5 (teorema fundamental). De esto se sigue que $+453R103$, y finalmente de esto $+453R1236$. Y es cierto que $453 \equiv 297^2 \pmod{1236}$

Sobre las formas lineales que contienen todos los números primos de los cuales un número dado cualquiera es un residuo o no residuo.

147.

Dado un número cualquiera A, pueden presentarse ciertas *fórmulas* bajo las cuales estarán contenidos todos los números primos a A de los cuales el residuo es A, o sea todos los que pueden ser *divisores* de los números de la forma $x^2 - A$ (denotando x^2 como un cuadrado indeterminado)*). Pero por brevedad examinaremos únicamente los divisores que son impares y primos a A, puesto que los restantes fácilmente pueden reducirse a este caso.

Primero, sea A o un número primo positivo de la forma $4n + 1$, o negativo de la forma $4n - 1$. Entonces, según el teorema fundamental, todos los números primos que, tomados positivamente, son residuos de A, serán divisores de $x^2 - A$; todos los números primos (excepto el número 2 que siempre es divisor), que son no residuos de A serán no divisores de $x^2 - A$. Denótense todos los residuos de A menores que A (excluyendo cero) por r, r', r'', etc.; todos los no residuos por n, n', n'', etc. Entonces cualquier número primo contenido en alguna de las formas $Ak + r$, $Ak + r'$, $Ak + r''$, etc. será divisor de $x^2 - A$, pero cualquier primo contenido en alguna de las formas $Ak + n$, $Ak + n'$, etc. será un no divisor, k es un número entero indeterminado. Llamamos *formas de los divisores de* $x^2 - A$ a las primeras, y *formas de los no divisores* a las segundas. El número de cada una de las dos será $\frac{1}{2}(A - 1)$. Ahora, si B es un número compuesto impar y ARB, todos los factores primos de B estarán contenidos en alguna de las primeras formas y por tanto lo estará B mismo. Por lo

*) De este modo, simplemente llamaremos a estos números los *divisores* de $x^2 - A$; es claro cuales son los *no divisores.*

que *cualquier* número impar contenido en una forma de los no divisores, será un no divisor de la forma $x^2 - A$. Pero este teorema no puede invertirse puesto que, si B es un no divisor compuesto impar de la forma $x^2 - A$, habrá entre los factores primos de B algunos no divisores. Si el número de ellos es *par,* B mismo se encontrará en alguna forma de los divisores. Véase art. 99.

Ejemplo. Para $A = -11$ se encuentran éstas : $11k + 1$, 3, 4, 5, 9 como las formas de los divisores de $x^2 + 11$, mientras que las formas de los no divisores serán $11k+2$, 6, 7, 8, 10. Por lo tanto, -11 será un no residuo de todos los números impares que están contenidos en algunas de las segundas formas, pero será un residuo de todos los primos pertenecientes a algunas de las primeras formas.

Se presentarán formas semejantes para divisores y no divisores de $x^2 - A$, donde A denota un número cualquiera. Pero se observa fácilmente que conviene considerar los valores de A que no sean divisibles por ningún cuadrado. En efecto, si $A = a^2A'$, todos los divisores*) de $x^2 - A$ también serán divisores de $x^2 - A'$, y de modo semejante los no divisores. Distinguiremos tres casos, 1) cuando A es de la forma $+(4n + 1)$ o $-(4n - 1)$. 2) cuando A es de la forma $-(4n + 1)$ o $+(4n - 1)$. 3) cuando A es par o sea de la forma $\pm(4n + 2)$.

148.

Primer caso, cuando A es de la forma $+(4n+1)$ o $-(4n-1)$. Resuélvase A en sus factores primos y asígnese a los que son de la forma $4n+1$ el signo positivo, y a los de la forma $4n - 1$, el signo negativo (de donde el producto de todos ellos será $= A$). Sean a, b, c, d, etc. estos factores. Distribúyanse todos los números menores que A y primos a A en dos clases: en la primera clase, todos los números que son no residuos o de ninguno de los números a, b, c, d, etc., o de dos, o de cuatro, o en general de un número par de ellos; en la segunda clase, los que son no residuos de uno de los números a, b, c, etc., o de tres etc., o generalmente de un número impar de ellos. Se denotarán los primeros por r, r', r'', etc.; los últimos por n, n', n'', etc. Entonces las formas $Ak + r$, $Ak + r'$, $Ak + r''$, etc. serán formas de los divisores de $x^2 - A$, y las formas $Ak + n$, $Ak + n'$, etc. serán formas de los no divisores de $x^2 - A$ (i.e., *un número primo cualquiera, aparte de* 2*, será divisor o no divisor de* $x^2 - A$ *según que esté contenido en alguna de las primeras formas o de las segundas respectivamente*). En efecto, si p es un número primo positivo y un residuo o no residuo de uno de

*) A saber, que sean primos a A.

los números a, b, c, etc., este mismo número será un residuo o un no residuo de p (teorema fundamental). Por lo tanto, si entre los números a, b, c, etc. hay m de los cuales p es un no residuo, otros tantos serán no residuos de p; de donde, si p está contenido en alguna de las primeras formas, m será par y ARp, pero si lo está en alguna de las últimas, m será impar y ANp.

Ejemplo. Sea $A = +105 = (-3)(+5)(-7)$. Entonces los números r, r', r'', etc. serán éstos: 1, 4, 16, 46, 64, 79 (que son no residuos de ninguno de los números 3, 5 y 7); 2, 8, 23, 32, 53, 92 (que son no residuos de los números 3 y 5); 26, 41, 59, 89, 101, 104 (que son no residuos de los números 3 y 7); 13, 52, 73, 82, 97, 103 (que son no residuos de los números 5 y 7). Los números n, n', n'', etc. serán éstos: 11, 29, 44, 71, 74, 86; 22, 37, 43, 58, 67, 88; 19, 31, 34, 61, 76, 94; 17, 38, 47, 62, 68, 83. Los primeros seis son no residuos de 3, los seis posteriores no residuos de 5, luego siguen los no residuos de 7 y finalmente los que son no residuos de todos los tres a la vez.

Se deduce fácilmente de la teoría de combinaciones y de los artículos 32 y 96, que el número de enteros r, r', r'', etc. será:

$$= t(1 + \frac{l(l-1)}{1 \cdot 2} + \frac{l(l-1)(l-2)(l-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \cdots)$$

el número de enteros n, n', n'', etc. será:

$$= t(l + \frac{l(l-1)(l-2)}{1 \cdot 2 \cdot 3} + \frac{l(l-1) \cdots (l-4)}{1 \cdot 2 \cdots 5} + \cdots)$$

donde l denota el número de enteros a, b, c, etc.;

$$t = 2^{-l}(a-1)(b-1)(c-1) \text{ etc.}$$

y se deben continuar ambas series hasta que se paren. (En efecto, se presentarán t números que son residuos de todos los a, b, c, etc., $\frac{t \cdot l(l-1)}{1 \cdot 2}$ que son no residuos de dos, etc., pero la brevedad no permite explicar esta demostración ampliamente). La suma*) de cada una de las series es $= 2^{l-1}$. De hecho, la primera proviene de ésta

$$1 + (l-1) + \frac{(l-1)(l-2)}{1 \cdot 2} + \cdots$$

sumando el segundo y tercer término, el cuarto y el quinto etc.; la segunda se deriva de esta misma, sumando el primer término y el segundo, el tercero y el cuarto etc. Por tanto se presentarán tantas formas divisores de $x^2 - A$ como se presentan formas no divisores, a saber $\frac{1}{2}(a-1)(b-1)(c-1)$ etc.

*) Desechado el factor t.

149.

Podemos contemplar a la vez el *segundo y tercer caso.* De hecho A siempre puede ponerse $= (-1)Q$, o $= (+2)Q$, o $= (-2)Q$, donde Q designa un número de la forma $+(4n+1)$, o $-(4n-1)$, los cuales consideramos en el artículo precedente. Sea en general $A = \alpha Q$ de manera que también $\alpha = -1$ o $\alpha = \pm 2$. Entonces A será un residuo de todos los números de los cuales ambos α y Q son residuos, o ambos no residuos; pero será un no residuo de todos los números de los cuales únicamente uno u otro de los números α y Q es un no residuo. De esto, las formas de los divisores y de los no divisores de $x^2 - A$ se derivan fácilmente. Si $\alpha = -1$, se distribuyen todos los números menores que $4A$ y primos al mismo en dos clases: en la primera, los que están en alguna forma de los divisores de $x^2 - Q$ y a la vez de la forma $4n+1$, junto con los que están en alguna forma de los no divisores de $x^2 - Q$ y al mismo tiempo de la forma $4n+3$; en la segunda, todos los demás. Sean los miembros de la primera clase r, r', r'', etc.; los de la segunda n, n', n'', etc. A será un residuo de todos los números primos contenidos en alguna de las formas $4Ak + r$, $4Ak + r'$, $4Ak + r''$, etc. y un no residuo de todos los números primos contenidos en alguna de las formas $4Ak + n$, $4Ak + n'$, etc. Si $\alpha = \pm 2$, distribúyanse todos los números menores que $8Q$ y primos al mismo, en dos clases: en la primera, los que están contenidos en alguna forma de los divisores de $x^2 - Q$ y a la vez en alguna de las formas $8n+1$ y $8n+7$ para el signo superior, o de las formas $8n+1$ y $8n+3$ para el inferior, junto con los que están contenidos en alguna forma de los no divisores de $x^2 - Q$ y al mismo tiempo en alguna de estas formas $8n+3$ y $8n+5$ para el signo superior, o de éstas $8n+5$ y $8n+7$ para el inferior; en la segunda clase, todos los demás. Entonces, denotados los números de la primera clase por r, r', r'', etc., y los números de la segunda clase por n, n', n'', etc., $\pm 2Q$ será un residuo de todos los números primos contenidos en alguna de las formas $8Qk + r$, $8Qk + r'$, $8Qk + r''$, etc.; pero un no residuo de todos los primos en alguna de las formas $8Qk + n$, $8Qk + n'$, $8Qk + n''$, etc. Además, puede demostrarse fácilmente que aquí también hay tantas formas divisores de $x^2 - A$ como no divisores.

Ejemplo. De este modo se encuentra que $+10$ es un residuo de todos los números primos contenidos en alguna de las formas $40k + 1$, 3, 9, 13, 27, 31, 37, 39; pero un no residuo de todos los primos contenidos en alguna de las formas $40k + 7$, 11, 17, 19, 21, 23, 29, 33.

150.

Estas formas tienen muchas propiedades bastante notables, de las cuales, sin embargo, indicamos únicamente una. Si B es un número compuesto, primo a A, tal que $2m$ de sus factores primos estén contenidos en alguna forma de los no divisores de $x^2 - A$, B estará contenido en alguna forma divisor de $x^2 - A$; pero si el número de factores primos de B contenidos en alguna forma de los no divisores de $x^2 - A$ es impar, B también estará contenido en una forma de los no divisores. Omitimos la demostración que no es difícil. De esto, sigue que no sólo cada número primo sino también todo número impar primo a A, que está contenido en alguna forma de los no divisores, será un no divisor, pues necesariamente algún factor primo de tal número debe ser un no divisor.

Sobre los trabajos de otros acerca de estas investigaciones.

151.

El teorema fundamental, que ha sido considerado como uno de los más elegantes de este género, no ha sido presentado hasta ahora en la forma tan simple como está enunciado arriba. Esto tiene que sorprendernos aún más; ya que otras proposiciones fundamentadas en él, de las cuales hubiera podido deducirse fácilmente el teorema, ya eran conocidas por el ilustre Euler. Sabía que existen ciertas formas en las cuales están contenidos todos los divisores primos de los números de la forma $x^2 - A$, y otras formas en las cuales están comprendidos todos los no divisores primos de los mismos números, de tal manera que unas excluyan las otras y había descubierto un método para hallar estas formas. Pero todos sus esfuerzos para hallar una demostración fueron en vano, y sólo dió un poco de validez a lo que había descubierto por inducción. En una memoria titulada *Novae demostrationes circa divisores numerorum formae* $xx + nyy$, que fue presentada en la academia de San Petersburgo el 20 de noviembre de 1775, y que fue conservada después de la muerte de este hombre ilustre en T. I. *Nov. Act.* de esta academia p. 47 y siguientes, parece haber creído que había logrado sus propósitos, pero se cometió un error. En efecto en la p. 65 está supuesto tácitamente que existen tales formas de los divisores y de los no divisores*), de donde no era difícil derivar *cuales* deben ser; pero el método que

*) A saber, existen números r, r', r'', etc., n, n', n'', etc., todos diferentes y $< 4A$ tales que todos los divisores primos de $x^2 - A$ estén contenidos en alguna de las formas $4Ak + r$, $4Ak + r'$, etc. y todos los no divisores primos en alguna de éstas $4Ak + n$, $4Ak + n'$, etc. (donde k es un número indeterminado).

él usó para comprobar esta proposición no parece idóneo. En otra obra, *De criteriis aequationis* $fxx + gyy = hzz$ *utrumque resolutionem admittat necne,* Opusc. Anal. T. I. (donde f, g, h son dados, x, y, z indeterminados) él descubrió por inducción que si la ecuación era resoluble para algún valor de $h = s$, también era resoluble para todo valor primo congruente a s según el módulo $4fg$. De esta proposición, la suposición sobre la cual hemos hablado puede demostrarse sin mucha dificultad. Pero la demostración de este teorema también eludió sus esfuerzos*), lo cual no es raro ya que a nuestro juicio se debía proceder a partir del teorema fundamental. Además, la verdad de esta proposición saldrá con espontaneidad de lo que enseñaremos en la siguiente sección.

Después de Euler, el gran Lagrange trabajó activamente en el mismo argumento en el distinguido tratado *Recherches d'analyse indéterminée,* Hist.de l'Ac. des Sc., 1785, p. 465 y los siguientes, donde llegó al teorema que si se observa es idéntico al teorema fundamental. En efecto, al designar p y q dos números primos positivos, los residuos absolutamente mínimos de las potencias $p^{\frac{q-1}{2}}$ y $q^{\frac{p-1}{2}}$ según los módulos q y p respectivamente serán ambos $+1$ o ambos -1 cuando p o q sea de la forma $4n + 1$. Pero cuando tanto p como q sean de la forma $4n + 3$, un residuo mínimo será $+1$, y el otro -1, p. 516, de lo que, según el artículo 106, se deriva que *la relación* (en el significado del art. 146) de p a q y de q a p es *la misma* cuando o p o q sea de la forma $4n + 1$; *la opuesta* cuando tanto p como q sean de la forma $4n + 3$. Esta proposición está contenida entre las proposiciones del artículo 131 y sigue también de las proposiciones 1, 3 y 9 del art. 133; alternativamente el teorema fundamental puede derivarse de ella. El gran Legendre también intentó una demostración, sobre la cual, puesto que es muy ingeniosa, hablaremos ampliamente en la siguiente sección. Sin embargo, ya que en ella se suponen muchas cosas sin demostración (como él mismo confiesa p. 520: *Nous avons supposé seulement* etc.), algunas de las cuales hasta ahora no han sido demostradas por nadie, y otras, según nuestro juicio, no pueden demostrarse sin el teorema fundamental mismo, parece que el método que siguió no se puede llevar a su fin, y que nuestra demostración tendrá que ser la primera. Además más abajo presentaremos *otras dos demostraciones* del

*) Como él mismo confiesa, l. c. p. 216: "Una demostración de este muy elegante teorema se desea todavía, aunque se ha investigado en vano durante mucho tiempo. Por tal razón será considerado excelentísimo el que tenga el éxito de encontrar la demostración de este teorema." Con cuánto ardor este hombre inmortal buscaba la demostración de este teorema y de otros que son solamente casos especiales del teorema fundamental, puede verse en muchos otros lugares, e.g., Opuscula Analytica, I, (*Additamentum ad Diss.* VIII) y II, (*Diss.* XIII) y en varias disertaciones en Comm. acad. Petrop. que hemos citado en varias ocasiones.

importante teorema, diferentes de la anterior y diferentes entre sí.

Sobre las congruencias no puras del segundo grado.

152.

Hasta este momento hemos tratado la congruencia pura $x^2 \equiv A \pmod{m}$ y hemos enseñado a determinar si es resoluble o no. La investigación de las *raíces mismas* se reduce por el artículo 105 al caso donde m o es primo o la potencia de un primo; pero el segundo por art. 101 se reduce al caso donde m es primo. Para este caso, lo que presentamos en el artículo 61 y siguientes junto con lo que enseñaremos en las Secciones V y VIII, comprende todo lo que puede hacerse por métodos directos. Sin embargo, éstos son infinitamente más prolijos donde son aplicables que los indirectos que enseñaremos en la Sección VI, y por tanto son memorables no tanto por su utilidad en la práctica sino por su propia belleza. *Las congruencias no puras del segundo grado* fácilmente pueden reducirse a las puras. Dada la congruencia

$$ax^2 + bx + c \equiv 0$$

para resolverse según el módulo m, equivaldrá a la congruencia

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}$$

i.e., cualquier número que satisfaga una de ellas también satisfará la otra. Pero esta segunda puede ponerse de la forma

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}$$

de donde todos los valores de $2ax + b$ menores que $4am$ pueden encontrarse si es que existen. Si designamos éstos por r, r', r'', etc., todas las soluciones de la congruencia propuesta podrán deducirse de las soluciones de las congruencias

$$2ax \equiv r - b, \quad 2ax \equiv r' - b, \quad \text{etc.} \pmod{4am}$$

las cuales aprendimos a encontrar en la Sección II. Además, observamos que la solución puede acortarse bastante mediante varios artificios; por ejemplo, en lugar de la congruencia propuesta puede encontrarse otra

$$a'x^2 + 2b'x + c' \equiv 0$$

que le sea equivalente, y en la cual a' divida a m; la brevedad no permite aquí explicarlo, pero puede referirse a la última sección.

Sección Quinta

SOBRE

LAS FORMAS Y LAS ECUACIONES INDETERMINADAS DE SEGUNDO GRADO.

Propósito de la investigación: definición y notación de las formas.

153.

En esta sección, trataremos principalmente las funciones de dos indeterminadas x e y de esta forma:

$$ax^2 + 2bxy + cy^2$$

donde a, b y c son enteros dados. Llamaremos a estas funciones *formas de segundo grado* o simplemente *formas.* En esta investigación se basa la resolución del famoso problema de encontrar todas las soluciones de cualquier ecuación indeterminada del segundo grado involucrando dos incógnitas, donde estas incógnitas pueden asumir tanto valores enteros como racionales. Este problema ciertamente ya fue resuelto por el ilustre Lagrange con toda generalidad. Además, muchos aspectos de la naturaleza *de las formas,* como la construcción de demostraciones, fueron encontrados tanto por este gran geómetra como por el ilustre Euler y antes por Fermat. Sin embargo, mediante una cuidadosa investigación de las formas, se nos presentaron tantos detalles nuevos que juzgamos valioso el trabajo de retomar completamente todo el argumento; primero, porque hemos conocido los descubrimientos difundidos en varios lugares por aquellos hombres, segundo, porque el método para tratar esto es, en su mayor parte, propio a nosotros, y, finalmente, porque nuestros nuevos hallazgos ciertamente no podrán comprenderse sin una exposición de los otros. Nos parece que no hay duda alguna de que muchos excelentes resultados de este género todavía están ocultos a

quienes se interesan en esta materia. Además, siempre presentaremos la historia de las proposiciones importantes en el lugar apropiado.

Cuando no nos conciernen las indeterminadas x e y, denotaremos por (a, b, c) a la forma $ax^2 + 2bxy + cy^2$. Por lo tanto, esta expresión denotará de manera indefinida una suma de tres partes: el producto del número dado a por un cuadrado indeterminado cualquiera, el producto del duplicado del número b por esta indeterminada y otra indeterminada, y el producto del número c por el cuadrado de esta segunda indeterminada. E.g., $(1, 0, 2)$ expresa la suma de un cuadrado y el duplicado de un cuadrado. Además, aunque las formas (a, b, c) y (c, b, a) denotan lo mismo, si sólo se consideran *sus términos,* difieren, sin embargo, si también prestamos atención al *orden.* Por esto las distinguiremos con cuidado en lo que sigue; más adelante se pondrá en claro lo que ganamos con esto.

Representación de los números; el determinante.

154.

Diremos que un número dado *se representa* por una forma dada si se puede dar valores enteros a las indeterminadas de la forma de modo que sea igual al número dado. Tendremos el siguiente:

TEOREMA. *Si el número M puede representarse por la forma (a, b, c) de manera que los valores de las indeterminadas, por los que esto se produce, son primos entre sí, entonces $b^2 - ac$ será un residuo cuadrático del número M.*

Demostración. Sean m y n los valores de las indeterminadas; i.e.,

$$am^2 + 2bmn + cn^2 = M$$

y tómense los números μ y ν de modo que sea $\mu m + \nu n = 1$ (art. 40). Entonces por multiplicación puede demostrarse fácilmente:

$$(am^2 + 2bmn + cn^2)(a\nu^2 - 2b\mu\nu + c\mu^2) \\ = (\mu(mb + nc) - \nu(ma + nb))^2 - (b^2 - ac)(m\mu + n\nu)^2$$

o sea

$$M(a\nu^2 - 2b\mu\nu + c\mu^2) = (\mu(mb + nc) - \nu(ma + nb))^2 - (b^2 - ac).$$

Por lo tanto será

$$b^2 - ac \equiv (\mu(mb + nc) - \nu(ma + nb))^2 \pmod{M}$$

i.e., $b^2 - ac$ será un residuo cuadrático de M.

Llamaremos al número $b^2 - ac$, de cuya índole dependen las propiedades de la forma (a, b, c), tal como lo enseñaremos en lo siguiente, el *determinante* de esta forma.

Los valores de la expresión $\sqrt{b^2 - ac} \pmod{M}$
a los cuales pertenece la representación del número M *por la forma* (a, b, c).

155.

Así

$$\mu(mb + nc) - \nu(ma + nb)$$

será un valor de la expresión

$$\sqrt{b^2 - ac} \pmod{M}$$

Pero es claro que los números μ y ν pueden determinarse de infinitas maneras de modo que $\mu m + \nu n = 1$, y así producirán unos y otros valores de esta expresión. Veremos qué relación tienen entre sí. Sea no sólo $\mu m + \nu n = 1$ sino también $\mu' m + \nu' n = 1$ y póngase

$$\mu(mb + nc) - \nu(ma + nb) = v, \quad \mu'(mb + nc) - \nu'(ma + nb) = v'.$$

Multiplicando la ecuación $\mu m + \nu n = 1$ por μ', la otra $\mu' m + \nu' n = 1$ por μ, y restando será $\mu' - \mu = n(\mu'\nu - \mu\nu')$, y al mismo tiempo multiplicando aquélla por ν' y ésta por ν, restando será $\nu' - \nu = m(\mu\nu' - \mu'\nu)$. De esto inmediatamente resulta

$$v' - v = (\mu'\nu - \mu\nu')(am^2 + 2bmn + cn^2) = (\mu'\nu - \mu\nu')M$$

o sea, $v' \equiv v \pmod{M}$. Por lo tanto, de cualquier modo que se determinen μ y ν, la fórmula $\mu(mb + nc) - \nu(ma + nb)$ no puede presentar valores *diferentes* (i.e., no congruentes) de la expresión $\sqrt{b^2 - ac} \pmod{M}$. Así pues, si v es un valor cualquiera de esta fórmula, diremos que la representación del número M por la forma

$ax^2 + 2bxy + cy^2$ donde $x = m$ e $y = n$, *pertenece al valor* v *de la expresión* $\sqrt{b^2 - ac}$ (mod. M). Además puede mostrarse fácilmente que, si algún valor de esta fórmula fuera v y $v' \equiv v \pmod{M}$, se puede tomar en lugar de los números μ y ν que dan v los otros μ' y ν' que dan v'. En efecto, si se hace

$$\mu' = \mu + \frac{n(v' - v)}{M}, \qquad \nu' = \nu - \frac{m(v' - v)}{M}$$

será

$$\mu' m + \nu' n = \mu m + \nu n = 1$$

y el valor de la fórmula producido por μ' y ν' excederá el valor producido por μ y ν en la cantidad $(\mu'\nu - \mu\nu')M$, que es $= (\mu m + \nu n)(v' - v) = v' - v$ o sea aquel valor será $= v'$.

156.

Si se tienen dos representaciones de un mismo número M por una misma forma (a, b, c) en las cuales las indeterminadas tienen valores primos entre sí, ellas pueden pertenecer o al mismo valor de la expresión $\sqrt{b^2 - ac} \pmod{M}$ o a valores diferentes. Sea

$$M = am^2 + 2bmn + cn^2 = am'^2 + 2bm'n' + cn'^2$$

y

$$\mu m + \nu n = 1, \quad \mu' m' + \nu' n' = 1$$

Es claro que si

$$\mu(mb + nc) - \nu(ma + nb) \equiv \mu'(m'b + n'c) - \nu'(m'a + n'b) \pmod{M}$$

entonces la congruencia siempre permanecerá válida, cualesquiera que sean los valores apropiados para μ y ν, μ' y ν'. En tal caso decimos que ambas representaciones pertenecen a un *mismo* valor de la expresión $\sqrt{b^2 - ac} \pmod{M}$; pero si la congruencia no vale para algunos valores de μ y ν, μ' y ν', no valdrá para ninguno, y diremos que las representaciones pertenecerán a valores *diferentes.* Pero si

$$\mu(mb + nc) - \nu(ma + nb) \equiv -(\mu'(m'b + n'c) - \nu'(m'a + n'b))$$

se dice que las representaciones pertenecen a valores *opuestos* de la expresión $\sqrt{b^2 - ac}$. También se usarán todas estas denominaciones cuando se tratan de varias representaciones de un mismo número por formas *diferentes,* pero que tienen el mismo determinante.

Ejemplo. Sea propuesta la forma $(3, 7, -8)$ cuyo determinante es $= 73$. Por esta forma se tendrán estas representaciones del número 57:

$$3 \cdot 13^2 + 14 \cdot 13 \cdot 25 - 8 \cdot 25^2; \quad 3 \cdot 5^2 + 14 \cdot 5 \cdot 9 - 8 \cdot 9^2$$

Para la primera, puede ponerse $\mu = 2$, $\nu = -1$ de donde resulta el valor de la expresión $\sqrt{73}$ (mod. 57) a la cual pertenece la representación

$$= 2(13 \cdot 7 - 25 \cdot 8) + (13 \cdot 3 + 25 \cdot 7) = -4$$

De modo semejante se descubrirá que la segunda representación, al hacer $\mu = 2$, $\nu = -1$, pertenece al valor $+4$. Por lo cual las dos representaciones pertenecen a valores opuestos.

Antes de proseguir, observamos que las formas de determinante $= 0$ están excluidas totalmente de las investigaciones siguientes. De hecho, ellas perturban únicamente la elegancia de los teoremas ya que exigen un tratamiento particular.

Una forma que implica otra o contenida en ella; la transformación propia e impropia.

157.

Si la forma F, cuyas indeterminadas son x e y, puede transmutarse en otra, F', cuyas indeterminadas son x' e y' por las sustituciones

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y'$$

de modo que α, β, γ, δ sean enteros; diremos que la primera *implica* la segunda o que la segunda *está contenida en la primera.* Sea F la forma

$$ax^2 + 2bxy + cy^2,$$

F' la forma

$$a'x'^2 + 2b'x'y' + cy'^2$$

y se tendrán las tres ecuaciones siguientes

$$\begin{aligned} a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2 \end{aligned}$$

Multiplicando la segunda ecuación por sí misma, la primera por la tercera, restando y removiendo las partes canceladas, resultará

$$b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2$$

De donde se deduce que el determinante de la forma F' es divisible por el determinante de la forma F y el cociente de ellos es un cuadrado. Por lo tanto es claro que estos determinantes tendrán el *mismo signo.* Además, si la forma F' puede transmutarse por una sustitución similar en la forma F, i.e., si tanto F' está contenida en F como F está contenida en F', los determinantes de las formas serán iguales*) y $(\alpha\delta - \beta\gamma)^2 = 1$. En este caso diremos que las formas son *equivalentes.* Por esto, para la equivalencia de formas, la igualdad de los determinantes es una condición necesaria, aunque aquélla no se deduzca sólo de ésta.— Llamaremos a la sustitución $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ una *transformación propia,* si $\alpha\delta - \beta\gamma$ es un número positivo, *impropia* si $\alpha\delta - \beta\gamma$ es negativo. Diremos que la forma F' está contenida en la forma F *propiamente* o *impropiamente* si F puede transmutarse en la forma F' por una transformación propia o impropia. Así si las formas F y F' son equivalentes, será $(\alpha\delta - \beta\gamma)^2 = 1$, así que si la transformación es propia, $\alpha\delta - \beta\gamma = 1$, si es impropia, $\alpha\delta - \beta\gamma = -1$. Si varias transformaciones son al mismo tiempo propias, o al mismo tiempo impropias, las llamaremos *semejantes;* sin embargo, una propia y una impropia se llaman *desemejantes.*

La equivalencia propia e impropia.

158.

Si los determinantes de las formas F y F' son iguales y si F' está contenida en F, entonces F estará contenida en F', propia o impropiamente, según que F' esté contenida en F propia o impropiamente.

Consideremos que F se transforma en F' poniendo

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y'$$

y F' se transformará en F poniendo

$$x' = \delta x - \beta y, \qquad y' = -\gamma x + \alpha y.$$

*) Es claro por el análisis anterior que esta proposición también es válida para formas cuyo determinante es $= 0$. Pero no se debe extender la ecuación $(\alpha\delta - \beta\gamma)^2 = 1$ a este caso.

En efecto, por esta sustitución resulta lo mismo de F' que de F al poner

$$x = \alpha(\delta x - \beta y) + \beta(-\gamma x + \alpha y), \qquad y = \gamma(\delta x - \beta y) + \delta(-\gamma x + \alpha y)$$

o sea

$$x = (\alpha\delta - \beta\gamma)x, \qquad y = (\alpha\delta - \beta\gamma)y$$

De esto queda manifiesto que F se hace $(\alpha\delta - \beta\gamma)^2 F$, i.e., de nuevo, F (artículo anterior). También está claro que la segunda transformación será propia o impropia, según que la primera sea propia o impropia.

Si tanto F' está contenida *propiamente* en F como F lo está en F', las llamaremos formas *propiamente equivalentes;* si alternativamente están contenidas impropiamente, las llamaremos *impropiamente equivalentes.*— En lo restante, se verá pronto el uso de estas distinciones.

Ejemplo. La forma $2x^2 - 8xy + 3y^2$ se cambia, por la sustitución $x = 2x' + y'$, $y = 3x' + 2y'$, en la forma $-13x'^2 - 12x'y' - 2y'^2$, y ésta se transforma en la primera mediante la sustitución $x' = 2x - y$, $y' = -3x + 2y$. Por lo que las formas $(2, -4, 3)$ y $(-13, -6, -2)$ son *propiamente equivalentes.*

Los problemas que ahora trataremos son éstos :

I. Propuestas dos formas cualesquiera que tienen el mismo determinante, se debe investigar si son equivalentes o no, si lo son propia o impropiamente o ambas (puesto que esto también puede suceder). Cuando tienen determinantes diferentes, se debe investigar por lo menos si la una implica la otra, propia o impropiamente o ambas. Finalmente, se debe hallar todas las transformaciones de la una en la otra, tanto las propias como las impropias.

II. Dada una forma cualquiera, se debe determinar si un número dado puede representarse por ella y determinar todas las representaciones. Pero, ya que las formas de determinante negativo requieren otros métodos diferentes que las formas de determinante positivo, primero trataremos lo común a los dos, y luego consideraremos cada género por separado.

Formas opuestas.

159.

Si la forma F implica la forma F', y ésta implica la forma F'', también la forma F implicará la forma F''.

Sean las indeterminadas de las formas F, F', F'', respectivamente x e y, x' e y', x'' e y'', y transfórmese F en F' al poner

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y'$$

y F' en F'' al poner

$$x' = \alpha' x'' + \beta' y'', \qquad y' = \gamma' x'' + \delta' y''$$

Es claro que F será transmutada en F'' al poner

$$x = \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y''), \qquad y = \gamma(\alpha' x'' + \beta' y'') + \delta(\gamma' x'' + \delta' y'')$$

o

$$x = (\alpha\alpha' + \beta\gamma')x'' + (\alpha\beta' + \beta\delta')y'', \qquad y = (\gamma\alpha' + \delta\gamma')x'' + (\gamma\beta' + \delta\delta')y''$$

Así F implicará F''.

Porque

$$(\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma') = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma')$$

será positivo si tanto $\alpha\delta - \beta\gamma$ como $\alpha'\delta' - \beta'\gamma'$ son positivos o ambos son negativos, y será negativo si uno de estos números es positivo y el otro negativo, la forma F implicará la forma F'' *propiamente* si F implica F' y F' a F'' del mismo modo, e *impropiamente* si es de modos diferentes.

De esto resulta que si se tienen las formas cualesquiera F, F', F'', F''', etc., cada una de las cuales implica la siguiente, la primera implicará la última *propiamente* si el número de formas que implican impropiamente a su sucesor es par, e *impropiamente* si este número es impar.

Si la forma F es equivalente a la forma F' y la forma F' es equivalente a la forma F'', entonces la forma F será equivalente a la forma F'' propiamente si la forma F equivale a la forma F' del mismo modo como la forma F' equivale a la forma F'', e impropiamente si son equivalencias de modos diferentes.

De hecho, ya que las formas F y F' son respectivamente equivalentes a las formas F' y F'', entonces aquéllas implicarán éstas, y así F implica a F'', tanto como las últimas implican a las primeras. Por lo tanto, F y F'' serán equivalentes. Pero se

sigue de lo anterior que F implicará F'' propiamente o impropiamente, según que la equivalencia de F y F', y F' y F'' sea del mismo modo o de modo diferente. De la misma manera F'' implicará F. Por lo tanto, F y F'' serán propiamente equivalentes en el primer caso, e impropiamente equivalentes en el segundo.

Las formas $(a, -b, c)$, (c, b, a), $(c, -b, a)$ *son equivalentes a la forma* (a, b, c), *con las dos primeras impropiamente, con la última propiamente.*

Ya que $ax^2 + 2bxy + cy^2$ se transforma en $ax'^2 - 2bx'y' + cy'^2$, al colocar $x = x' + 0 \cdot y'$, $y = 0 \cdot x' - y'$, esta transformación es impropia pues $(1)(-1) - (0)(0) = -1$; pero se transforma en $cx'^2 + 2bx'y' + ay'^2$ por la transformación impropia $x = 0 \cdot x' + y'$, $y = x' + 0 \cdot y'$; y en la forma $cx'^2 - 2bx'y' + ay'^2$ por la transformación propia $x = 0 \cdot x' - y'$, $y = x' + 0 \cdot y'$.

De esto queda claro que cualquier forma equivalente a la forma (a, b, c) equivaldrá *propiamente* o a ella misma o a la forma $(a, -b, c)$. Al mismo tiempo, si tal forma implica la forma (a, b, c) o está contenida en ella misma, ella implicará la forma (a, b, c) o la forma $(a, -b, c)$ *propiamente* o estará contenida *propiamente* en una de las dos. Llamaremos a (a, b, c) y $(a, -b, c)$ formas *opuestas.*

Formas contiguas.

160.

Si las formas (a, b, c) y (a', b', c') tienen el mismo determinante, y si además $c = a'$ y $b \equiv -b' \pmod{c}$, o sea $b + b' \equiv 0 \pmod{c}$, llamaremos a estas formas *contiguas.* Cuando es necesaria una determinación más exacta, diremos que la primera es contigua *a la parte primera* de la segunda, la segunda *a la parte última* de la primera.

Así, por ejemplo, la forma $(7, 3, 2)$ es contigua a la parte última de la forma $(3, 4, 7)$; la forma $(3, 1, 3)$ a ambas partes de su opuesta $(3, -1, 3)$.

Formas contiguas siempre son propiamente equivalentes. En efecto la forma $ax^2 + 2bxy + cy^2$ se transforma en su contigua por la sustitución $x = -y'$, $y = x' + \frac{b+b'}{c}y'$ (la cual es propia porque $0 \cdot (\frac{b+b'}{c}) - (1 \cdot -1) = 1$), como se demuestra fácilmente con la ayuda de la ecuación $b^2 - ac = b'^2 - cc'$, donde por hipótesis $\frac{b+b'}{c}$ es un entero. Por otra parte, estas definiciones y conclusiones no valen si $c = a' = 0$. Pero este caso no puede ocurrir aquí más que en formas cuyo determinante es un cuadrado.

Las formas (a, b, c) y (a', b', c') son propiamente equivalentes si $a = a'$, $b \equiv b' \pmod{a}$. En efecto, la forma (a, b, c) equivale propiamente a la forma $(c, -b, a)$

(artículo anterior), pero esta última será contigua a la parte primera de la forma (a', b', c').

Divisores comunes de los coeficientes de las formas.

161.

Si la forma (a, b, c) implica la forma (a', b', c'), cualquier divisor común de los números a, b y c también dividirá a los números a', b' y c' y cada divisor común de los números a, $2b$ y c dividirá a a', $2b'$ y c'.

De hecho, si la forma $ax^2 + 2bxy + cy^2$ mediante la sustitución $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ se transforma en la forma $a'x'^2 + 2b'x'y' + c'y'^2$, se tendrán estas ecuaciones:

$$a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a'$$
$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b'$$
$$a\beta^2 + 2b\beta\delta + c\delta^2 = c'$$

de donde se sigue la proposición (para la segunda parte de la proposición, en lugar de la segunda ecuación se usa $2a\alpha\beta + 2b(\alpha\delta + \beta\gamma) + 2c\gamma\delta = 2b'$.)

De esto se deduce que el máximo común divisor de los números a, $b\,(2b)$, c divide al máximo común divisor de los números a', $b'\,(2b')$, c'. Si además la forma (a', b', c') implica la forma (a, b, c), i.e., si las formas son equivalentes, el máximo común divisor de los números a, $b\,(2b)$, c será igual al máximo común divisor de los números a', $b'\,(2b')$, c', puesto que tanto aquél debe dividir a éste, como éste a aquél. Por eso, si en este caso a, $b\,(2b)$, c no tienen un divisor común, i.e., si el máximo común divisor $= 1$, tampoco tendrá a', $b'\,(2b')$, c' un divisor común.

El nexo de todas las transformaciones semejantes de una forma dada en otra forma.

162.

Problema. *Si la forma*

$$AX^2 + 2BXY + CY^2 \ldots F$$

implica la forma

$$ax^2 + 2bxy + cy^2 \ldots f$$

y si se da alguna transformación de la primera en la segunda: de ésta se deducen todas las transformaciones restantes semejantes a esta misma.

Solución. Sea la transformación dada $X = \alpha x + \beta y$, $Y = \gamma x + \delta y$. Supongamos primero que la otra semejante a ésta es $X = \alpha' x + \beta' y$, $Y = \gamma' x + \delta' y$, de donde investigaremos lo siguiente. Dados los determinantes de las formas F y f $= D$ y d y $\alpha\delta - \beta\gamma = e$, $\alpha'\delta' - \beta'\gamma' = e'$, tendremos (art. 157) $d = De^2 = De'^2$, y puesto que por hipótesis e y e' tienen los mismos signos, $e = e'$. Se tendrán así las siguientes seis ecuaciones:

$$A\alpha^2 + 2B\alpha\gamma + C\gamma^2 = a \tag{1}$$
$$A\alpha'^2 + 2B\alpha'\gamma' + C\gamma'^2 = a \tag{2}$$
$$A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta = b \tag{3}$$
$$A\alpha'\beta' + B(\alpha'\delta' + \beta'\gamma') + C\gamma'\delta' = b \tag{4}$$
$$A\beta^2 + 2B\beta\delta + C\delta^2 = c \tag{5}$$
$$A\beta'^2 + 2B\beta'\delta' + C\delta'^2 = c \tag{6}$$

Si por brevedad denotamos los números

$$A\alpha\alpha' + B(\alpha\gamma' + \gamma\alpha') + C\gamma\gamma'$$
$$A(\alpha\beta' + \beta\alpha') + B(\alpha\delta' + \beta\gamma' + \gamma\beta' + \delta\alpha') + C(\gamma\delta' + \delta\gamma')$$
$$A\beta\beta' + B(\beta\delta' + \delta\beta') + C\delta\delta'$$

por a', $2b'$, c', de las ecuaciones precedentes deduciremos otras nuevas*)

$$a'^2 - D(\alpha\gamma' - \gamma\alpha')^2 = a^2 \tag{7}$$
$$2a'b' - D(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') = 2ab \tag{8}$$
$$4b'^2 - D((\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 + 2ee') = 2b^2 + 2ac$$

de donde resulta, sumando $2Dee' = 2d = 2b^2 - 2ac$

$$4b'^2 - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 = 4b^2 \tag{9}$$
$$a'c' - D(\alpha\delta' - \gamma\beta')(\beta\gamma' - \delta\alpha') = b^2$$

*) Estas ecuaciones se originan así: la (7) viene de $(1)\cdot(2)$ (i.e., si la ecuación (1) se multiplica por la ecuación (2), o mejor, si la parte primera de la primera se multiplica por la parte primera de la segunda, y la parte última de la primera por la parte última de la segunda, y luego se ponen iguales los productos). La (8) viene de $(1)\cdot(4) + (2)\cdot(3)$; la siguiente, la cual no está numerada de $(1)\cdot(6) + (2)\cdot(5) + (3)\cdot(4) + (3)\cdot(4)$; la siguiente, sin número, de $(3)\cdot(4)$; la (11) de $(3)\cdot(6) + (4)\cdot(5)$; la (12) de $(5)\cdot(6)$. Siempre usaremos una notación semejante en lo siguiente. Pero debemos dejar los cálculos a los lectores.

de donde, restando $D(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = b^2 - ac$ se tiene

$$a'c' - D(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta') = ac \tag{10}$$

$$2b'c' - D(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta') = 2bc \tag{11}$$

$$c'^2 - D(\beta\delta' - \delta\beta')^2 = c^2 \tag{12}$$

Ahora supongamos que el máximo común divisor de los números a, $2b$, c es m, y los números $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ determinados de tal manera que

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$$

(art. 40). Multiplíquense las ecuaciones (7), (8), (9), (10), (11), (12) respectivamente por $\mathfrak{A}^2$, $2\mathfrak{A}\mathfrak{B}$, $\mathfrak{B}^2$, $2\mathfrak{A}\mathfrak{C}$, $2\mathfrak{B}\mathfrak{C}$, $\mathfrak{C}^2$ y súmense los productos. Ahora si por brevedad ponemos

$$\mathfrak{A}a' + 2\mathfrak{B}b' + \mathfrak{C}c' = T \tag{13}$$

$$\mathfrak{A}(\alpha\gamma' - \gamma\alpha') + \mathfrak{B}(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha') + \mathfrak{C}(\beta\delta' - \delta\beta') = U \tag{14}$$

donde claramente T y U serán enteros, resultará

$$T^2 - DU^2 = m^2$$

Así llegamos a esta conclusión elegante: *de dos transformaciones semejantes cualesquiera de la forma F en f se deduce la resolución de la ecuación indeterminada $t^2 - Du^2 = m^2$ en enteros,* es decir $t = T$, $u = U$. Además como en nuestros razonamientos no hemos supuesto que las transformaciones son *diferentes, una* transformación tal considerada dos veces debe producir una solución. Entonces, por razón de que $\alpha' = \alpha$, $\beta' = \beta$, etc., será $a' = a$, $b' = b$, $c' = c$, por tanto $T = m$, $U = 0$, que es una solución obvia por sí misma.

Ahora, primero consideremos conocidas una transformación y una solución de la ecuación indeterminada, y luego investiguemos cómo puede deducirse la otra transformación y cómo α', β', γ', δ' dependen de α, β, γ, δ, T, U. Para este fin, multiplicamos primero la ecuación (1) por $\delta\alpha' - \beta\gamma'$, la (2) por $\alpha\delta' - \gamma\beta'$, la (3) por $\alpha\gamma' - \gamma\alpha'$, la (4) por $\gamma\alpha' - \alpha\gamma'$ y sumamos los productos, de donde resultará

$$(e + e')a' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')a \tag{15}$$

De modo semejante, de

$$(\delta\beta' - \beta\delta')((1) - (2)) + (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')((3) + (4)) + (\alpha\gamma' - \gamma\alpha')((5) - (6))$$

se tiene

$$2(e + e')b' = 2(\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')b \tag{16}$$

Finalmente, de $(\delta\beta' - \beta\delta')((3) - (4)) + (\alpha\delta' - \gamma\beta')(5) + (\delta\alpha' - \beta\gamma')(6)$ resultará

$$(e + e')c' = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')c \tag{17}$$

Sustituyendo estos valores ((15), (16), (17)) en la (13) se obtiene

$$(e + e')T = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)$$

o

$$2eT = (\alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha')m \tag{18}$$

de donde T puede deducirse con más facilidad que de la (13). — Combinando esta ecuación con (15), (16), (17) se obtiene $ma' = Ta$, $2mb' = 2Tb$, $mc' = Tc$. Sustituyendo estos valores de a', $2b'$, c' en las ecuaciones (7)–(12) y escribiendo $m^2 + DU^2$ en lugar de T^2 después de las alteraciones necesarias se transforman en éstas:

$$\begin{aligned}
(\alpha\gamma' - \gamma\alpha')^2 m^2 &= a^2U^2 \\
(\alpha\gamma' - \gamma\alpha')(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')m^2 &= 2abU^2 \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')^2 m^2 &= 4b^2U^2 \\
(\alpha\gamma' - \gamma\alpha')(\beta\delta' - \delta\beta')m^2 &= acU^2 \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')(\beta\delta' - \delta\beta')m^2 &= 2bcU^2 \\
(\beta\delta' - \delta\beta')^2 m^2 &= c^2U^2
\end{aligned}$$

De esto con la ayuda de la ecuación (14) y de $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, se deduce fácilmente (multiplicando la primera, la segunda y la cuarta; la segunda, la tercera y la quinta; la cuarta, la quinta y la sexta respectivamente por $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ y sumando los productos):

$$\begin{aligned}
(\alpha\gamma' - \gamma\alpha')Um^2 &= maU^2 \\
(\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')Um^2 &= 2mbU^2 \\
(\beta\delta' - \delta\beta')Um^2 &= mcU^2
\end{aligned}$$

y de esto, dividiendo por mU*)

$$aU = (\alpha\gamma' - \gamma\alpha')m \tag{19}$$
$$2bU = (\alpha\delta' + \beta\gamma' - \gamma\beta' - \delta\alpha')m \tag{20}$$
$$cU = (\beta\delta' - \delta\beta')m \tag{21}$$

de tales ecuaciones puede deducirse algún U con más facilidad que de la (14). — De modo semejante se concluye que no importa cómo se determinen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ (porque puede ser de infinitas maneras diferentes), tanto T como U tomarán el mismo valor.

Ahora si la ecuación (18) se multiplica por α, la (19) por 2β, la (20) por $-\alpha$, la suma da

$$2aeT + 2(\beta a - \alpha b)U = 2(\alpha\delta - \beta\gamma)\alpha' m = 2e\alpha' m.$$

De modo semejante de $\beta(18) + \beta(20) - 2\alpha(21)$

$$2\beta eT + 2(\beta b - \alpha c)U = 2(\alpha\delta - \beta\gamma)\beta' m = 2e\beta' m$$

Además de $\gamma(18) + 2\delta(19) - \gamma(20)$ es

$$2\gamma eT + 2(\delta a - \gamma b)U = 2(\alpha\delta - \beta\gamma)\gamma' m = 2e\gamma' m$$

Finalmente, de $\delta(18) + \delta(20) - 2\gamma(21)$ resulta

$$2\delta eT + 2(\delta b - \gamma c)U = 2(\alpha\delta - \beta\gamma)\delta' m = 2e\delta' m$$

Si en estas fórmulas se sustituyen para a, b, c sus valores de (1), (3), (5) se obtiene

$$\alpha' m = \alpha T - (\alpha B + \gamma C)U$$
$$\beta' m = \beta T - (\beta B + \delta C)U$$
$$\gamma' m = \gamma T + (\alpha A + \gamma B)U$$
$$\delta' m = \delta T + (\beta A + \delta B)U\dagger)$$

*) Esto no se permitiría si $U = 0$: pero entonces la verdad de las ecuaciones (19), (20), (21) se obtendría inmediatamente de la primera, la tercera, y la sexta de las anteriores.

Del análisis anterior se deduce que no existe ninguna transformación semejante de la forma F en la f que no esté contenida en la fórmula

$$X = \frac{1}{m}(\alpha t - (\alpha B + \gamma C)u)x + \frac{1}{m}(\beta t - (\beta B + \delta C)u)y$$
$$Y = \frac{1}{m}(\gamma t + (\alpha A + \gamma B)u)x + \frac{1}{m}(\delta t + (\beta A + \delta B)u)y \qquad (I)$$

donde t y u denotan números enteros indeterminados que satisfacen la ecuación $t^2 - Du^2 = m^2$. De esto no hemos podido concluir que todos los valores de t y u que satisfacen aquella ecuación proporcionarán transformaciones adecuadas al sustituirlos en la fórmula (I). Sin embargo,

1. Por medio de las ecuaciones (1), (3), (5) y $t^2 - Du^2 = m^2$, puede confirmarse fácilmente que la forma F siempre puede transformarse en la forma f por una sustitución proveniente de valores cualesquiera de t y u. Por brevedad, suprimimos un cálculo más prolijo que difícil.

2. Cada trasformación deducida de la fórmula será semejante a la propuesta porque

$$\frac{1}{m}(\alpha t-(\alpha B+\gamma C)u)\cdot\frac{1}{m}(\delta t+(\beta A+\delta B)u)-\frac{1}{m}(\beta t-(\beta B+\delta C)u)\cdot\frac{1}{m}(\gamma t+(\alpha A+\gamma B)u)$$
$$= \frac{1}{m^2}(\alpha\delta - \beta\gamma)(t^2 - Du^2) = \alpha\delta - \beta\gamma$$

3. Si las formas F y f tienen determinantes diferentes, puede ocurrir que la fórmula (I) para algunos valores de t y u produzca sustituciones que impliquen *fracciones:* éstas deben rechazarse. Todas las restantes serán transformaciones adecuadas y no existirán otras.

4. Si las formas F y f tienen el mismo determinante, y por tanto son *equivalentes,* la fórmula (I) no presentará ninguna transformación que implique

†) De esto se deduce fácilmente

$$AeU = (\delta\gamma' - \gamma\delta')m$$
$$2BeU = (\alpha\delta' - \delta\alpha' + \gamma\beta' - \beta\gamma')m$$
$$CeU = (\beta\alpha' - \alpha\beta')m$$

fracciones, de donde en este caso dará la solución completa del problema. Esto lo demostramos como sigue:

Del teorema del artículo anterior, resulta en este caso que m será un común divisor de los números $A, 2B$ y C. Ya que $t^2 - Du^2 = m^2$, es $t^2 - B^2u^2 = m^2 - ACu^2$, por lo que $t^2 - B^2u^2$ será divisible por m^2: de esto también $4t^2 - 4B^2u^2$, y por lo tanto (porque $2B$ es divisible por m) también $4t^2$ por m^2, y por eso $2t$ por m. De esto $\frac{2}{m}(t + Bu)$ y $\frac{2}{m}(t - Bu)$ serán enteros, y ambos son pares o ambos impares (ya que la diferencia entre ellos, $\frac{4}{m}Bu$, es par). Si ambos fueran impares, también su producto sería impar, pero ya que el cuádruplo del número $\frac{1}{m^2}(t^2 - B^2u^2)$, el cual hemos mostrado como entero, es necesariamente par; entonces este caso es imposible, y por tanto $\frac{2}{m}(t+Bu)$ y $\frac{2}{m}(t-Bu)$ son siempre pares, de donde $\frac{1}{m}(t+Bu)$ y $\frac{1}{m}(t-Bu)$ serán enteros. De esto se deduce sin dificultad que los cuatro coeficientes en la (I) son siempre enteros. *Q. E. D.*

De lo anterior se concluye que, si se tienen todas las soluciones de la ecuación $t^2 - D^2u^2 = m^2$, se derivarán todas las transformaciones de la forma (A, B, C) en (a, b, c) semejantes a la transformación dada. Desde luego, enseñaremos a encontrar estas soluciones en lo siguiente. Observamos que el número de soluciones es siempre finito cuando D es negativo o un cuadrado positivo; pero es infinito cuando D es positivo y no un cuadrado. Cuando se presenta este caso, y cuando D no es $= d$ (ver arriba 3), se debe investigar cuidadosamente la manera en que se puedan conocer *a priori* los valores de t y u que producen sustituciones libres de fracciones. Pero para este caso, expondremos más adelante otro método libre de este problema.

Ejemplo. La forma $x^2 + 2y^2$ se transforma por la sustitución propia $x = 2x' + 7y', y = x' + 5y'$ en la forma (6, 24, 99): se desean *todas* las transformaciones propias de la primera en la segunda. Aquí $D = -2, m = 3$, y por lo tanto la ecuación por resolverse es: $t^2 + 2u^2 = 9$. Ella se satisface de seis maneras diferentes poniendo $t = 3, -3, 1, -1, 1, -1; u = 0, 0, 2, 2, -2, -2$ respectivamente. La tercera y sexta resolución dan sustituciones en fracciones, por lo que deben rechazarse. De los restantes resultan cuatro sustituciones:

$$x = \begin{vmatrix} 2x' + 7y' \\ -2x' - 7y' \\ -2x' - 9y' \\ 2x' + 9y' \end{vmatrix} \qquad y = \begin{vmatrix} x' + 5y' \\ -x' - 5y' \\ x' + 3y' \\ -x' - 3y' \end{vmatrix}$$

de las cuales la primera es la propuesta.

Formas ambiguas.

163.

Ya hemos dicho que puede ser que alguna forma F implique otra tanto propia como impropiamente. Es claro que esto ocurre si entre las formas F y F' pudiera interponerse otra, G, de modo que F implique G, G implique F', y la forma G sea impropiamente equivalente consigo misma. Si, en efecto, se supone que F implica G propia o impropiamente: como G implica a G impropiamente, F implicará a G impropia o propiamente respectivamente y, por tanto, en los dos casos tanto propia como impropiamente (art. 159). Del mismo modo, no importa la forma en que se suponga que G implica F', F siempre debe implicar F' tanto propia como impropiamente. En el caso obvio donde el término medio de la forma es $= 0$, se ve que tales formas son impropiamente equivalentes a sí mismas. De hecho, tal forma será opuesta a sí misma (art. 159) y por lo tanto impropiamente equivalente. En general cada forma (a, b, c) en la cual $2b$ es divisible por a está provista de esta propiedad. En efecto, la forma (c, b, a) será contigua (art. 160) a la primera parte de ésta y propiamente equivalente a ella. Sin embargo, (c, b, a) por art. 159 es impropiamente equivalente a la forma (a, b, c); por lo que (a, b, c) equivaldrá a sí misma impropiamente. Llamaremos *ambiguas* a tales formas (a, b, c) en las cuales $2b$ es divisible por a.

Así tendremos este teorema:

La forma F implicará la forma F' tanto propia como impropiamente, si puede encontrarse una forma ambigua contenida en F que implica a F'. Es evidente que esta proposición también puede invertirse:

Teorema sobre el caso en que una forma está contenida en otra al mismo tiempo propia e impropiamente.

164.

Teorema. *Si la forma*

$$Ax^2 + 2Bxy + Cy^2 \qquad (F)$$

implica la forma

$$A'x'^2 + 2B'x'y' + C'y'^2 \qquad (F')$$

tanto propia como impropiamente, entonces puede encontrarse una forma ambigua contenida en F y que implica a F'.

Supongamos que la forma F se transforma en la forma F' tanto por la sustitución

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y'$$

como por ésta diferente a ella

$$x = \alpha' x' + \beta' y', \qquad y = \gamma' x' + \delta' y'$$

Entonces, denotados los números $\alpha\delta - \beta\gamma$ y $\alpha'\delta' - \beta'\gamma'$ por e y e' se tendrá $B'^2 - A'C' = e^2(B^2 - AC) = e'^2(B^2 - AC)$; de esto $e^2 = e'^2$, y, ya que por la hipótesis e y e' tienen signos opuestos, $e = -e'$ o $e + e' = 0$. Es claro que si en F' para x' se sustituye $\delta' x'' - \beta' y''$, y para y', $-\gamma' x'' + \alpha' y''$ se producirá la misma forma como cuando en la F se escribe

o bien	1)	para x	$\alpha(\delta' x'' - \beta' y'') + \beta(-\gamma' x'' + \alpha' y'')$	
		i.e.	$(\alpha\delta' - \beta\gamma')x'' + (\beta\alpha' - \alpha\beta')y''$	
		y para y	$\gamma(\delta' x'' - \beta' y'') + \delta(-\gamma' x'' + \alpha' y'')$	
		i.e.	$(\gamma\delta' - \delta\gamma')x'' + (\delta\alpha' - \gamma\beta')y''$	
o bien	2)	para x	$\alpha'(\delta' x'' - \beta' y'') + \beta'(-\gamma' x'' + \alpha' y'')$	i.e., $e' x''$
		y para y	$\gamma'(\delta' x'' - \beta' y'') + \delta'(-\gamma' x'' + \alpha' y'')$	i.e., $e' y''$

Así pues, denotados los números $\alpha\delta' - \beta\gamma'$, $\beta\alpha' - \alpha\beta'$, $\gamma\delta' - \delta\gamma'$, $\delta\alpha' - \gamma\beta'$ por a, b, c, d, la forma F se transformará en la misma forma por las dos sustituciones

$$x = ax'' + by'', \quad y = cx'' + dy''; \qquad x = e'x'', \quad y = e'y'',$$

de donde obtendremos las siguientes tres ecuaciones:

$$Aa^2 + 2Bac + Cc^2 = Ae'^2 \tag{1}$$

$$Aab + B(ad + bc) + Ccd = Be'^2 \tag{2}$$

$$Ab^2 + 2Bbd + Cd^2 = Ce'^2 \tag{3}$$

Pero de los mismos valores de a, b, c, d se encuentra:

$$ad - bc = ee' = -e^2 = -e'^2 \tag{4}$$

De aquí y de $d(1) - c(2)$

$$(Aa + Bc)(ad - bc) = (Ad - Bc)e'^2$$

y por tanto

$$A(a+d) = 0$$

Además, de $(a+d)(2) - b(1) - c(3)$ se tiene

$$(Ab + B(a+d) + Cc)(ad - bc) = (-Ab + B(a+d) - Cc)e'^2$$

y por lo tanto

$$B(a+d) = 0$$

Finalmente de $a(3) - b(2)$ obtenemos

$$(Bb + Cd)(ad - bc) = (-Bb + Ca)e'^2$$

y por lo tanto

$$C(a+d) = 0$$

Por esto, como no todos A, B, C pueden ser $= 0$, será necesario que $a + d = 0$, o $a = -d$.

De $a(2) - b(1)$ tenemos

$$(Ba + Cc)(ad - bc) = (Ba - Ab)e'^2$$

de donde

$$Ab - 2Ba - Cc = 0. \tag{5}$$

De las ecuaciones $e + e' = 0$, $a + d = 0$, o

$$\alpha\delta - \beta\gamma + \alpha'\delta' - \beta'\gamma' = 0, \qquad \alpha\delta' - \beta\gamma' - \gamma\beta' + \delta\alpha' = 0$$

resulta $(\alpha + \alpha')(\delta + \delta') = (\beta + \beta')(\gamma + \gamma')$ o

$$(\alpha + \alpha') : (\gamma + \gamma') = (\beta + \beta') : (\delta + \delta').$$

Sea la razón*) $m : n$ igual a esta razón con números mínimos, de modo que m y n sean primos entre sí, y se toman μ, ν de manera que $\mu m + \nu n = 1$. Además sea r el

*) Si todos $\alpha + \alpha', \gamma + \gamma', \beta + \beta', \delta + \delta'$ fueran $= 0$, la razón sería indeterminada, y por ende el método no aplicable. Pero con cuidado se puede mostrar que esto no puede darse con nuestras suposiciones; pues sería $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma'$ i.e. $e = e'$, porque $e = -e', e = e' = 0$. También $B'^2 - A'C'$, i.e. el determinante de la forma F' sería $= 0$. Tales formas las hemos excluido por completo.

máximo común divisor de los números a, b, c, cuyo cuadrado divida a^2+bc, o $bc-ad$, o e^2; por lo que r también dividirá a e. Determinado esto así, si se supone que la forma F se transforma por la sustitución

$$x = mt + \frac{\nu e}{r}u, \qquad y = nt - \frac{\mu e}{r}u$$

en la forma $Mt^2 + 2Ntu + Pu^2 \quad (G)$, ésta será ambigua e implicará la forma F'.

Demostración. I. Para que sea evidente que la forma G es ambigua, mostraremos

$$M(b\mu^2 - 2a\mu\nu - c\nu^2) = 2Nr$$

de donde, ya que r divide a a, b, c, entonces $\frac{1}{r}(b\mu^2 - 2a\mu\nu - c\nu^2)$ será un entero, y por lo tanto $2N$ un múltiplo de M. De hecho tenemos:

$$M = Am^2 + 2Bmn + Cn^2, \qquad Nr = (Am\nu - B(m\mu - n\nu) - Cn\mu)e \tag{6}$$

Además se confirma mediante cálculos fáciles que

$$\begin{aligned} 2e + 2a = e - e' + a - d &= (\alpha - \alpha')(\delta + \delta') - (\beta - \beta')(\gamma + \gamma') \\ 2b &= (\alpha + \alpha')(\beta - \beta') - (\alpha - \alpha')(\beta + \beta') \end{aligned}$$

De esto, puesto que $m(\gamma + \gamma') = n(\alpha + \alpha')$, $m(\delta + \delta') = n(\beta + \beta')$ será

$$\begin{aligned} m(2e + 2a) &= -2nb \qquad \text{o} \\ me + ma + nb &= 0 \end{aligned} \tag{7}$$

Del mismo modo encontramos que

$$\begin{aligned} 2e - 2a = e - e' - a + d &= (\alpha + \alpha')(\delta - \delta') - (\beta + \beta')(\gamma - \gamma') \\ 2c &= (\gamma - \gamma')(\delta + \delta') - (\gamma + \gamma')(\delta - \delta') \end{aligned}$$

y de esto $n(2e - 2a) = -2mc$ o

$$ne - na + mc = 0 \tag{8}$$

Ahora si se suma $m^2(b\mu^2 - 2a\mu\nu - c\nu^2)$ a

$$(1-m\mu-n\nu)(m\nu(e-a)+(m\mu+1)b)+(me+ma+nb)(m\mu\nu+\nu)+(ne-na+mc)m\nu^2$$

que evidentemente $= 0$ pues

$$1 - \mu m - \nu n = 0, \qquad me + ma + nb = 0, \qquad ne - na + mc = 0$$

al desarrollar los productos y remover las partes canceladas, resulta $2m\nu e + b$. Por lo cual será

$$m^2(b\mu^2 - 2a\mu\nu - c\nu^2) = 2m\nu e + b \tag{9}$$

Del mismo modo sumando a $mn(b\mu^2 - 2a\mu\nu - c\nu^2)$ lo siguiente:

$$(1-m\mu-n\nu)((n\nu-m\mu)e-(1+m\mu+n\nu)a)-(me+ma+nb)m\mu^2+(ne-na+mc)n\nu^2$$

se encuentra

$$mn(b\mu^2 - 2a\mu\nu - c\nu^2) = (n\nu - m\mu)e - a \tag{10}$$

Finalmente sumando a $n^2(b\mu^2 - 2a\mu\nu - c\nu^2)$ lo siguiente:

$$(m\mu+n\nu-1)(n\mu(e+a)+(n\nu+1)c)-(me+ma+nb)n\mu^2-(ne-na+mc)(n\mu\nu+\mu)$$

obtenemos

$$n^2(b\mu^2 - 2a\mu\nu - c\nu^2) = -2n\mu e - c \tag{11}$$

Ahora se deduce de la (9), la (10) y la (11) que

$$\begin{aligned}(Am^2 + 2Bmn + Cn^2)&(b\mu^2 - 2a\mu\nu - c\nu^2)\\ &= 2e(Am\nu + B(n\nu - m\mu) - Cn\mu) + Ab - 2Ba - Cc\end{aligned}$$

o por la (6),

$$M(b\mu^2 - 2a\mu\nu - c\nu^2) = 2Nr. \qquad \textit{Q. E. D.}$$

II. Para demostrar que la forma G implica la forma F', demostraremos *primero*, que G se transforma en F' al poner

$$t = (\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y', \qquad u = \frac{r}{e}(n\alpha - m\gamma)x' + \frac{r}{e}(n\beta - m\delta)y' \qquad (S)$$

segundo, que $\frac{r}{e}(n\alpha - m\gamma)$ y $\frac{r}{e}(n\beta - m\delta)$ son enteros.

1. Puesto que F se transforma en G al ponerse

$$x = mt + \frac{\nu e}{r}u, \quad y = nt - \frac{\mu e}{r}u$$

la forma G se transformará por la sustitución (S) en la misma forma en que se transforma F al ponerse

$$x = m((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') + \nu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$

i.e., $$= \alpha(m\mu + n\nu)x' + \beta(m\mu + n\nu)y' \quad \text{o} \quad = \alpha x' + \beta y'$$

y $$y = n((\mu\alpha + \nu\gamma)x' + (\mu\beta + \nu\delta)y') - \mu((n\alpha - m\gamma)x' + (n\beta - m\delta)y')$$

i.e., $$= \gamma(n\nu + m\mu)x' + \delta(n\nu + m\mu)y' \quad \text{o} \quad = \gamma x' + \delta y'$$

Mediante esta sustitución F se transforma en F'; por lo tanto G se transformará en F' por la sustitución (S).

2. De los valores de e, b y d se encuentra $\alpha' e + \gamma b - \alpha d = 0$, o, ya que $d = -a$, $n\alpha' e + n\alpha a + n\gamma b = 0$; de esto, usando la (7), $n\alpha' e + n\alpha a = m\gamma e + m\gamma a$ o

$$(n\alpha - m\gamma)a = (m\gamma - n\alpha')e \tag{12}$$

Además, $\alpha n b = -\alpha m(e + a)$, $\gamma m b = -m(\alpha' e + \alpha a)$ y por lo tanto

$$(n\alpha - m\gamma)b = (\alpha' - \alpha)me \tag{13}$$

Finalmente, $\gamma' e - \gamma a + \alpha c = 0$; de esto multiplicando por n y sustituyendo para na su valor de (8) obtenemos

$$(n\alpha - m\gamma)c = (\gamma - \gamma')ne \tag{14}$$

De modo semejante se saca $\beta' e + \delta b - \beta d = 0$ ó sea $n\beta' e + n\delta b + n\beta a = 0$, y, por lo tanto, por la (7), $n\beta' e + n\beta a = m\delta e + m\delta a$ o

$$(n\beta - m\delta)a = (m\delta - n\beta')e \tag{15}$$

Además $\beta n b = -\beta m(e + a)$, $\delta m b = -m(\beta' e + \beta a)$ y por tanto

$$(n\beta - m\delta)b = (\beta' - \beta)me \tag{16}$$

Finalmente $\delta' e - \delta a + \beta c = 0$; de esto multiplicando por n y sustituyendo na por suvalor de la (8):

$$(n\beta - m\delta)c = (\delta - \delta')ne \tag{17}$$

Ahora, como el máximo común divisor de los números a, b, c es r, pueden encontrarse enteros $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ de modo que

$$\mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c = r$$

Hecho esto, de la (12), la (13), la (14); la (15), la (16) y la (17) se obtiene

$$\mathfrak{A}(m\gamma - n\alpha') + \mathfrak{B}(\alpha' - \alpha)m + \mathfrak{C}(\gamma - \gamma')n = \frac{r}{e}(n\alpha - m\gamma)$$
$$\mathfrak{A}(m\delta - n\beta') + \mathfrak{B}(\beta' - \beta)m + \mathfrak{C}(\delta - \delta')n = \frac{r}{e}(n\beta - m\delta)$$

y por lo tanto $\frac{r}{e}(n\alpha - m\gamma)$, $\frac{r}{e}(n\beta - m\delta)$ son enteros. *Q. E. D.*

165.

Ejemplo. La forma $3x^2+14xy-4y^2$ se transforma en $-12x'^2-18x'y'+39y'^2$, tanto propiamente, con poner

$$x = 4x' + 11y', \qquad y = -x' - 2y',$$

como impropiamente, con poner

$$x = -74x' + 89y', \qquad y = 15x' - 18y'$$

Aquí, por lo tanto, $\alpha + \alpha'$, $\beta + \beta'$, $\gamma + \gamma'$, $\delta + \delta'$ son -70, 100, 14, -20; y $-70 : 14 = 100 : -20 = 5 : -1$. Así, pongamos $m = 5$, $n = -1$, $\mu = 0$, $\nu = -1$. Los números a, b, c son -237, -1170, 48, de los cuales el máximo común divisor $= 3 = r$; finalmente $e = 3$. De esto la transformación (S) será $x = 5t - u$, $y = -t$. Por ella la forma $(3, 7, -4)$ se transforma en la forma ambigua $t^2 - 16tu + 3u^2$.

Si las formas F y F' son equivalentes, entonces la forma G contenida en la forma F también estará contenida en F'. Sin embargo, puesto que también implica la misma forma F', será equivalente a ella y por tanto también a la forma F. Por lo tanto, en este caso el teorema se enuncia así:

Si F y F' son equivalentes tanto propia como impropiamente, podrá encontrarse una forma ambigua equivalente a las dos. Además en este caso $e = \pm 1$, y por lo tanto r que divide a e, será $= 1$.

Lo anterior es suficiente acerca de la transformación de las formas en general; así que pasaremos a la consideración de *las representaciones.*

Generalidades sobre las representaciones de los números por las formas y su nexo con las transformaciones.

166.

Si la forma F implica la forma F', cualquier número que puede representarse por F' también podrá ser representado por F.

Sean x e y, x' e y' las indeterminadas de las formas F y F' respectivamente, y supongamos que se representa al número M por F'. Al hacer $x' = m$ e $y' = n$, la forma F se transforma en F' por la sustitución

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

Entonces, evidentemente, si se pone

$$x = \alpha m + \beta n, \quad y = \gamma m + \delta n$$

F se transforma en M.

Si M puede representarse de varias maneras por la forma F', e.g. poniendo $x' = m'$ e $y' = n'$, seguirán varias representaciones de M por F. De hecho, si fuera tanto

$$\alpha m + \beta n = \alpha m' + \beta n' \quad \text{como} \quad \gamma m + \delta n = \gamma m' + \delta n'$$

sería o bien $\alpha\delta - \beta\gamma = 0$, y por lo tanto también el determinante de la forma $F = 0$ (contrariamente a la hipótesis), o bien $m = m'$, $n = n'$. De esto resulta que M puede representarse al menos de tantas maneras diferentes por F como por F'.

Por ende, si tanto F implica F' como F' implica F i.e., si F y F' son equivalentes, y el número M puede representarse por una de las dos, también puede representarse por la otra, de tantas maneras diferentes para la una como para la otra.

Finalmente, observamos que en este caso el máximo común divisor de los números m y n es igual al máximo común divisor de los números $\alpha m + \beta n$ y $\gamma m + \delta n$. Sea aquél $= \Delta$, y tomemos los números μ y ν de modo que resulte $\mu m + \nu n = \Delta$. Entonces, tendremos

$$(\delta\mu - \gamma\nu)(\alpha m + \beta n) - (\beta\mu - \alpha\nu)(\gamma m + \delta n) = (\alpha\delta - \beta\gamma)(\mu m + \nu n) = \pm\Delta$$

De esto, el máximo común divisor de los números $\alpha m + \beta n$ y $\gamma m + \delta n$ dividirá a Δ, y también Δ lo dividirá a él; pues, evidentemente dividirá a $\alpha m + \beta n$ y $\gamma m + \delta n$. Por lo que, necesariamente aquél será $= \Delta$. Por lo tanto, cuando m y n son primos entre sí, también $\alpha m + \beta n$ y $\gamma m + \delta n$ lo serán.

167.

TEOREMA. *Si las formas*

$$ax^2 + 2bxy + cy^2 \qquad (F)$$
$$a'x'^2 + 2b'x'y' + c'y'^2 \qquad (F')$$

son equivalentes, el determinante de ellas $= D$*, y la última se transforma en la primera al poner*

$$x' = \alpha x + \beta y, \quad y' = \gamma x + \delta y$$

y si además el número M *se representa por* F*, escribiendo* $x = m$*,* $y = n$*, y, por lo tanto, por* F' *haciendo*

$$x' = \alpha m + \beta n = m', \quad y' = \gamma m + \delta n = n'$$

de modo que m *sea primo a* n *y por tanto también* m' *a* n'*, entonces ambas representaciones pertenecerán o al mismo valor de la expresión* $\sqrt{D} \pmod{M}$ *o a valores opuestos según que la transformación de la forma* F' *en* F *sea propia o impropia.*

Demostración. Se determinarán los números μ y ν de manera que resulte $\mu m + \nu n = 1$ y póngase

$$\frac{\delta\mu - \gamma\nu}{\alpha\delta - \beta\gamma} = \mu', \quad \frac{-\beta\mu + \alpha\nu}{\alpha\delta - \beta\gamma} = \nu'$$

(los cuales serán enteros pues $\alpha\delta - \beta\gamma = \pm 1$). Entonces tendremos

$$\mu' m' + \nu' n' = 1. \quad \text{(cf. final del artículo anterior)}$$

Además sea

$$\mu(bm + cn) - \nu(am + bn) = V, \quad \mu'(b'm' + c'n') - \nu'(a'm' + b'n') = V'$$

y V y V' serán valores de la expresión $\sqrt{D} \pmod{M}$ a los cuales pertenecen la primera y la segunda representaciones. Si en V' para μ', ν', m', n' se sustituyen los valores de ellos, pero en V

$$\begin{aligned} &\text{para } a, && a'\alpha^2 + 2b'\alpha\gamma + c'\gamma^2 \\ &\text{para } b, && a'\alpha\beta + b'(\alpha\delta + \beta\gamma) + c'\gamma\delta \\ &\text{para } c, && a'\beta^2 + 2b'\beta\delta + c'\delta^2 \end{aligned}$$

se encontrará por cálculo que $V = V'(\alpha\delta - \beta\gamma)$.

Por esto tendremos o bien $V = V'$ o $V = -V'$ según que $\alpha\delta - \beta\gamma = +1$ o $= -1$, i.e., las representaciones pertenecerán al mismo valor de la expresión $\sqrt{D}$ (mod. M) o a los valores opuestos, según que la transformación de F' en F sea propia o impropia. *Q. E. D.*

Si de esta manera se tienen varias representaciones del número M por la forma (a, b, c) por medio de valores primos entre sí de las indeterminadas pertenecientes a valores *diferentes* de la expresión $\sqrt{D}$ (mod. M), entonces las representaciones correspondientes por la forma (a', b', c') pertenecerán a los mismos valores respectivos. Si no existe representación alguna del número M por ninguna forma perteneciente a un cierto valor del determinante, tampoco existirá ninguna otra perteneciente a este valor y equivalente a él.

168.

TEOREMA. *Si el número M se representa por la forma $ax^2 + 2bxy + cy^2$, asignando los valores m y n primos entre sí a x e y, y si el valor de la expresión $\sqrt{D}$* (mod. M)*, al cual pertenece esta representación, es N, entonces las formas (a, b, c) y $(M, N, \frac{N^2-D}{M})$ serán propiamente equivalentes.*

Demostración. Es claro que, por el artículo 155, pueden encontrarse números enteros μ y ν de modo que

$$m\mu + n\nu = 1, \quad \mu(bm + cn) - \nu(am + bn) = N.$$

Usando esto, la forma (a, b, c) se transforma mediante la sustitución $x = mx' - \nu y'$ e $y = nx' + \mu y'$, la cual claramente es propia, en una forma cuyo determinante es $= D(m\mu + n\nu)^2$, i.e., $= D$, o en una forma equivalente. Tal forma, si se pone $= (M', N', \frac{N'^2-D}{M'})$, será,

$$M' = am^2 + 2bmn + cn^2 = M, \quad N' = -m\nu a + (m\mu - n\nu)b + n\mu c = N.$$

Por lo que la forma en la cual se transforma (a, b, c) por esta transformación será $(M, N, \frac{N^2-D}{M})$. *Q. E. D.*

Además, de las ecuaciones

$$m\mu + n\nu = 1, \quad \mu(mb + nc) - \nu(ma + nb) = N$$

se deduce

$$\mu = \frac{nN + ma + nb}{am^2 + 2bmn + cn^2} = \frac{nN + ma + nb}{M}, \quad \nu = \frac{mb + nc - mN}{M}$$

las cuales serán, por lo tanto, números enteros.

Además, hay que notar que esta proposición no vale si $M = 0$; pues el término $\frac{N^2 - D}{M}$ será indeterminado*).

169.

Si se tienen varias representaciones del número M por (a, b, c) pertenecientes al mismo valor N de la expresión $\sqrt{D} \pmod{M}$ (donde siempre suponemos que los valores de x e y son primos entre sí), también se deducirán varias transformaciones propias de la forma $(a, b, c) \ldots (F)$ en $(M, N, \frac{N^2 - D}{M}) \ldots (G)$. De hecho, si tal representación proviene de los valores $x = m'$ e $y = n'$, (F) también se transforma en (G) por la sustitución

$$x = m'x' + \frac{m'N - m'b - n'c}{M}y', \quad y = n'x' + \frac{n'N + m'a + n'b}{M}y'.$$

Viceversa, de cada transformación propia de la forma (F) en (G), se deriva una representación del número M por la forma (F) perteneciente al valor N. Si (F) se transforma en (G), al poner $x = mx' - \nu y'$ e $y = nx' + \mu y'$, entonces M se representa por (F) al poner $x = m$ e $y = n$, y puesto que aquí $m\mu + n\nu = 1$, el valor de la expresión $\sqrt{D} \pmod{M}$, al cual pertenece la representación, será $\mu(bm + cn) - \nu(am + bn)$, i.e., N. De varias transformaciones propias y diferentes resulta el mismo número de representaciones diversas pertenecientes a N†). De esto

*) De hecho, si deseamos extender la terminología a este caso, podemos decir que si N es el valor de la expresión $\sqrt{D} \pmod{M}$, o sea $N^2 \equiv D \pmod{M}$, significará que $N^2 - D$ es un múltiplo de M, y por lo tanto $= 0$.

†) Si se supone que la misma representación proviene de dos transformaciones propias diferentes, ellas tendrán que ser:

$$1)\, x = mx' - \nu y', \quad y = nx' + \mu y'; \qquad 2)\, x = mx' - \nu' y', \quad y = nx' + \mu' y'$$

Sin embargo, de las dos ecuaciones

$$m\mu + n\nu = m\mu' + n\nu', \quad \mu(mb + nc) - \nu(ma + nb) = \mu'(mb + nc) - \nu'(ma + nb)$$

se deduce fácilmente que o bien $M = 0$ o bien $\mu = \mu'$, $\nu = \nu'$. Pero ya hemos excluído a $M = 0$.

se concluye fácilmente que, si se tuvieran todas las transformaciones propias de la forma (F) en la (G), resultarán de éstas todas las representaciones de M por (F) pertenecientes al valor N. De donde, la cuestión de investigar las representaciones de un número dado por una forma dada (en la cual se dan valores primos entre sí a las indeterminadas) se reduce a la cuestión de investigar todas las transformaciones propias de esta forma en la forma equivalente dada.

Ahora, aplicando a ésta lo que aprendimos en el artículo 162, se colige con facilidad que si la representación de algún número M por la forma (F) perteneciente al valor N es ésta $x = \alpha$ e $y = \gamma$; la fórmula general que comprende todas las representaciones del mismo número por la forma (F) perteneciente al valor N será:

$$x = \frac{\alpha t - (\alpha b + \gamma c)u}{m}, \quad y = \frac{\gamma t + (\alpha a + \gamma b)u}{m}$$

donde m es el máximo común divisor de los números a, $2b$, c, y t y u representan todos los números que satisfacen la ecuación $t^2 - Du^2 = m^2$.

170.

Si la forma (a, b, c) es equivalente a alguna forma ambigua y por lo tanto equivalente a la forma $(M, N, \frac{N^2-D}{M})$, tanto propia como impropiamente, o propiamente equivalente a las formas $(M, N, \frac{N^2-D}{M})$ y $(M, -N, \frac{N^2-D}{M})$, se tendrán las representaciones del número M por la forma (F) perteneciente tanto al valor N como al valor $-N$. Y recíprocamente, si se tienen varias representaciones del número M por la misma forma (F) pertenecientes a valores *opuestos* N y $-N$ de la expresión $\sqrt{D}$ (mod. M), la forma (F) será equivalente a la forma (G) tanto propia como impropiamente y podrá encontrarse una forma ambigua a la cual sea equivalente (F).

Estas generalidades sobre las representaciones son suficientes por ahora. Hablaremos más adelante sobre las representaciones en las cuales las indeterminadas tienen valores no primos entre sí. En lo que atañe a las otras propiedades, las formas cuyo determinante es negativo deben ser tratadas de modo totalmente diferente que las formas de determinante positivo; por lo tanto consideraremos ahora las dos por separado. Así, comenzamos con las más fáciles.

Sobre las formas de un determinante negativo.

171.

PROBLEMA. *Dada una forma cualquiera (a, b, a'), cuyo determinante nega-*

tivo $= -D$*, donde* D *es un número positivo, se debe encontrar una forma* (A, B, C) *propiamente equivalente a ésta, en la cual* A *no es mayor que* $\sqrt{\frac{4}{3}D}$*, ni mayor que* C*, ni menor que* $2B$*.*

Resolución. Suponemos que en la forma dada no valen a la vez las tres condiciones; de lo contrario no sería necesario buscar otra forma. Sea b' el menor residuo absoluto del número $-b$ según el módulo a'*), y $a'' = \frac{b'^2+D}{a'}$, el cual será un entero; ya que $b'^2 \equiv b^2$, $b'^2 + D \equiv b^2 + D \equiv aa' \equiv 0 \pmod{a'}$. Si $a'' < a'$, resulta de nuevo que b'' es el menor residuo absoluto de $-b'$, según el módulo a'', y $a''' = \frac{b''^2+D}{a''}$. Si de nuevo $a''' < a''$ sea de nuevo b''' el menor residuo absoluto de $-b''$ según el módulo a''', y sea $a'''' = \frac{b'''^2+D}{a'''}$. Esta operación continuará, hasta llegar en la progresión a', a'', a''', a'''' etc., a un término $a^{(m+1)}$, el cual no es menor que su antecedente $a^{(m)}$. Esto debe ocurrir finalmente, ya que se tendría una progresión infinita de números enteros decrecientes. Entonces la forma $(a^{(m)}, b^{(m)}, a^{(m+1)})$ satisfará todas las condiciones.

Demostración. I. En la progresión de formas (a, b, a'), (a', b', a''), (a'', b'', a''') etc., cada una es contigua a su antecedente; por lo cual la última será propiamente equivalente a la primera (artículos 159 y 160).

II. Como $b^{(m)}$ es el residuo menor absoluto de $-b^{(m-1)}$, según el módulo $a^{(m)}$, no será mayor que $\frac{1}{2}a^{(m)}$ (art. 4).

III. Ya que $a^{(m)}a^{(m+1)} = D + b^{(m)}b^{(m)}$ y $a^{(m+1)}$ no es $< a^{(m)}$, tampoco será $a^{(m)}a^{(m)} > D + b^{(m)}b^{(m)}$ y como $b^{(m)}$ no es $> \frac{1}{2}a^{(m)}$, tampoco será $> D + \frac{1}{4}a^{(m)}a^{(m)}$ y $\frac{3}{4}a^{(m)}a^{(m)}$ no será $> D$ y finalmente $a^{(m)}$ no $> \sqrt{\frac{4}{3}D}$.

Ejemplo. Dada la forma (304, 217, 155) cuyo determinante $= -31$, se encuentra la progresión de las formas:

$$(304, 217, 155), \quad (155, -62, 25), \quad (25, 12, 7), \quad (7, 2, 5), \quad (5, -2, 7)$$

La última es la buscada. Del mismo modo, para la forma $(121, 49, 20)$ cuyo determinante $= -19$, se encuentran las equivalentes $(20, -9, 5)$, $(5, -1, 4)$, $(4, 1, 5)$: por lo que $(4, 1, 5)$ será la forma buscada.

---

*) Conviene observar que, si el primer o el último término a ó a' de alguna forma dada (a, b, a') fuera $= 0$, su determinante sería un cuadrado positivo; por lo cual esto no puede ocurrir en este caso. Por la misma razón no pueden existir signos opuestos de los términos de ambos lados a y a' para la forma de un determinante negativo.

Llamaremos *formas reducidas* a tales formas (A, B, C) cuyo determinante es negativo y en las cuales A ni es mayor que $\sqrt{\frac{4}{3}D}$, ni mayor que C, ni menor que $2B$. Por lo que para cada forma de un determinante negativo podremos encontrar una forma reducida propiamente equivalente a ella.

172.

PROBLEMA. *Encontrar las condiciones bajo las cuales dos formas reducidas no idénticas* (a, b, c) *y* (a', b', c') *con el mismo determinante,* $-D$*, puedan ser propiamente equivalentes.*

Resolución. Supongamos, lo cual es posible, que a' no es $> a$, y que la forma $ax^2 + 2bxy + cy^2$ se transforma en $a'x'^2 + 2b'x'y' + c'y'^2$ por la sustitución propia $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$. Entonces se tendrán las siguientes ecuaciones

$$a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a' \tag{1}$$

$$a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b' \tag{2}$$

$$\alpha\delta - \beta\gamma = 1 \tag{3}$$

De la (1) resulta $aa' = (a\alpha + b\gamma)^2 + D\gamma^2$; por lo cual aa' será positivo; y como $ac = D + b^2$, $a'c' = D + b'^2$, también serán positivos ac y $a'c'$; por lo tanto todos a, a', c, c' tendrán el mismo signo. Pero, ni a ni a' es $> \sqrt{\frac{4}{3}D}$ y, por tanto, tampoco aa' es $> \frac{4}{3}D$; por lo cual mucho menos puede ser $D\gamma^2 (= aa' - (a\alpha + b\gamma)^2)$ mayor que $\frac{4}{3}D$. De esto, γ será o $= 0$, o $= \pm 1$.

I. Si $\gamma = 0$, se deduce de la (3) que o bien son $\alpha = 1, \delta = 1$, o $\alpha = -1, \delta = -1$. En ambos casos, resulta de la (1) que $a' = a$, y de la (2) que $b' - b = \pm\beta a$. Pero, b no es $> \frac{1}{2}a$ ni $b' > \frac{1}{2}a'$ y tampoco $> \frac{1}{2}a$. Por consiguiente, la ecuación $b' - b = \pm\beta a$ no puede darse, a no ser que sea

o bien $b = b'$, de donde resultaría $c' = \frac{b'^2 + D}{a'} = \frac{b^2 + D}{a} = c$; por lo que las formas (a, b, c), (a', b', c') serían idénticas (contrariamente a la hipótesis),

o bien $b = -b' = \pm\frac{1}{2}a$. En este caso, también sería $c' = c$ y la forma (a', b', c') sería $(a, -b, c)$, i.e., la forma opuesta a (a, b, c). Al mismo tiempo, es evidente que estas formas serían ambiguas ya que $2b = \pm a$.

II. Si $\gamma = \pm 1$, de la (1) resulta $a\alpha^2 + c - a' = \pm 2b\alpha$. Pero c no es menor que a, y por lo tanto no menor que a'; de esto $a\alpha^2 + c - a'$, ó sea $2b\alpha$ no es menor que $a\alpha^2$. Por lo que, como $2b$ no es mayor que a, tampoco α será menor que α^2; de donde necesariamente $\alpha = 0$, ó $= \pm 1$.

1) Si $\alpha = 0$, de la (1) tenemos $a' = c$, y puesto que a ni es mayor que c, ni menor que a', será necesariamente $a' = a = c$. Además de la (3) tenemos que $\beta\gamma = -1$ de donde de la (2) $b + b' = \pm\delta c = \pm\delta a$. De modo semejante a como se dedujo de la (I) tendremos:

o bien $b = b'$, en tal caso las formas serían idénticas (contrariamente a la hipótesis),

o bien $b = -b'$, en tal caso las formas (a, b, c), (a', b', c') serían opuestas.

2) Si $\alpha = \pm 1$, resulta de la (1) que $\pm 2b = a + c - a'$. Por lo tanto como ni a ni $c < a'$, tampoco sería $2b < a$ ni $< c$. Pero, $2b$ ni es $> a$, ni $> c$, de donde necesariamente $\pm 2b = a = c$, y de la ecuación $\pm 2b = a + c - a'$ será también $= a'$. Por lo tanto de la (2) resulta que

$$b' = a(\alpha\beta + \gamma\delta) + b(\alpha\delta + \beta\gamma)$$

o, puesto que $\alpha\delta - \beta\gamma = 1$,

$$b' - b = a(\alpha\beta + \gamma\delta) + 2b\beta\gamma = a(\alpha\beta + \gamma\delta \pm \beta\gamma)$$

por lo cual necesariamente como antes

o bien $b = b'$, de donde las formas (a, b, c) y (a', b', c') son idénticas (contrariamente a la hipótesis),

o bien $b = -b'$, y, por tanto, aquellas formas son opuestas. A la vez, en este caso las formas serían ambiguas; ya que $a = \pm 2b$.

De todo esto se concluye que las formas (a, b, c) y (a', b', c') no pueden ser propiamente equivalentes, a no ser que fueran opuestas, y al mismo tiempo *o bien* ambiguas *o bien* $a = c = a' = c'$. En estos casos, pudo verse fácilmente que las formas (a, b, c) y (a', b', c') son propiamente equivalentes. De hecho, si las formas son impropiamente opuestas y, además ambiguas, también tendrán que ser propiamente equivalentes. Si $a = c$, la forma $(\frac{D+(a-b)^2}{a}, a - b, a)$ será contigua a la forma (a, b, c) y por ende será equivalente; pero puesto que $D + b^2 = ac = a^2$ es $\frac{D+(a-b)^2}{a} = 2a - 2b$, la forma $(2a - 2b, a - b, a)$ es ambigua; por lo cual (a, b, c) también equivaldrá a su opuesta propiamente.

Igualmente, ahora puede deducirse fácilmente que cuando dos formas reducidas (a, b, c) y (a', b', c') son no opuestas pueden ser impropiamente equivalentes. En efecto serán impropiamente equivalentes si (a, b, c) y $(a', -b', c')$, las cuales no son idénticas, son propiamente equivalentes, y viceversa. Es evidente que la condición

bajo la cual aquéllas sean impropiamente equivalentes es que sean idénticas además de ser ambiguas o que $a = c$. Las formas reducidas que no son ni idénticas ni opuestas tampoco pueden ser propia ni impropiamente equivalentes.

173.

PROBLEMA. *Dadas dos formas F y F', con el mismo determinante negativo, se debe investigar si son equivalentes.*

Resolución. Búsquense dos formas reducidas f y f' propiamente equivalentes a las formas F y F' respectivamente. Si las formas f y f' son propiamente o impropiamente equivalentes, o equivalentes de ambos modos, entonces F y F' también lo son; pero si f y f' no son equivalentes de ninguna manera, tampoco lo son F y F'.

Del artículo anterior pueden presentarse cuatro casos:

1) Si f y f' no son ni idénticas ni opuestas, tampoco F y F' serían equivalentes de ningún modo.

2) Si f y f' son, *primero*, o idénticas u opuestas y, *segundo*, o ambiguas, o tienen sus términos extremos iguales, F y F' serían tanto propia como impropiamente equivalentes.

3) Si f y f' son idénticas, pero ni son ambiguas ni tienen términos extremos iguales, F y F' sólo serían propiamente equivalentes.

4) Si f y f' son opuestas, pero ni son ambiguas ni tienen términos extremos iguales, F y F' sólo serían impropiamente equivalentes.

Ejemplo. Para las formas $(41, 35, 30)$ y $(7, 18, 47)$ cuyo determinante $= -5$, se encuentran las formas reducidas no equivalentes $(1, 0, 5)$ y $(2, 1, 3)$; por lo que las formas originales de ningún modo serán equivalentes. A las formas $(23, 38, 63)$ y $(15, 20, 27)$ equivale la misma forma reducida $(2, 1, 3)$, y como ella es al mismo tiempo ambigua, las formas $(23, 38, 63)$ y $(15, 20, 27)$ serán equivalentes tanto propia como impropiamente. A las formas $(37, 53, 78)$ y $(53, 73, 102)$ equivalen las formas reducidas $(9, 2, 9)$ y $(9, -2, 9)$, y puesto que éstas son opuestas y sus términos extremos iguales, las formas dadas serán equivalentes propia e impropiamente a la forma opuesta.

174.

El número de formas reducidas que tienen un determinante dado $-D$ siempre es finito y relativamente pequeño en relación con el número D. Estas mismas

formas pueden encontrarse mediante dos métodos. Denotaremos las formas reducidas indefinidas del determinante $-D$ por (a, b, c) donde deben determinarse todos los valores de a, b, c.

Primer método. Tómense para a todos los números positivos y negativos no mayores que $\sqrt{\frac{4}{3}D}$, de los cuales $-D$ sea un residuo cuadrático, y para cada a se hace b sucesivamente igual a todos los valores de la expresión $\sqrt{-D} \pmod{a}$, no mayores que $\frac{1}{2}a$, tomados tanto positiva como negativamente; para cada uno de los valores determinados de a y b se pone $c = \frac{D+b^2}{a}$. Si resultan de este modo unas formas en las cuales $c < a$, éstas deberán rechazarse, pero las restantes son claramente reducidas.

Segundo método. Tómense para b todos los números positivos y negativos, no mayores que $\frac{1}{2}\sqrt{\frac{4}{3}D}$ o sea $\sqrt{\frac{1}{3}D}$. Para cada b, resuélvase $b^2 + D$ de todas las maneras como pueda hacerse en dos factores menores que $2b$ (también debe tomarse en cuenta la diversidad de los signos). Cuando los factores son diferentes, póngase el menor factor $= a$ y el otro $= c$. Como a no es $> \sqrt{\frac{4}{3}D}$, todas las formas originadas de esta manera serán claramente reducidas. Finalmente es claro que no puede existir ninguna forma reducida que no se encuentre por ambos métodos.

Ejemplo. Sea $D = 85$. Aquí el límite de los valores de a es $\sqrt{\frac{340}{3}}$, que está entre 10 y 11. Los números entre 1 y 10 (inclusive), de los cuales -85 es residuo cuadrático, son 1, 2, 5 y 10. De aquí se tienen doce formas:
$(1, 0, 85)$, $(2, 1, 43)$, $(2, -1, 43)$, $(5, 0, 17)$, $(10, 5, 11)$, $(10, -5, 11)$; $(-1, 0, -85)$, $(-2, 1, -43)$, $(-2, -1, -43)$, $(-5, 0, -17)$, $(-10, 5, -11)$, $(-10, -5, -11)$.

Con el otro método, se tiene $\sqrt{\frac{85}{3}}$ para el límite de los valores de b, el cual está situado entre 5 y 6. Para $b = 0$, resultan las formas

$$(1, 0, -85), \quad (-1, 0, -85), \quad (5, 0, 17), \quad (-5, 0, -17),$$

para $b = \pm 1$ resultan $(2, \pm 1, 43)$ y $(-2, \pm 1, -43)$.
Para $b = \pm 2$ no existe ninguna, ya que 89 no puede resolverse en dos factores de los cuales sean ambos < 4. Lo mismo vale para ± 3 y ± 4. Finalmente para $b = \pm 5$ resultan

$$(10, \pm 5, 11) \quad \text{y} \quad (-10, \pm 5, -11).$$

175.

Si se rechaza una u otra de dos formas no idénticas pero propiamente equivalentes entre todas las formas reducidas de un determinante dado, las formas

restantes estarán provistas de esta propiedad notable: que cualquier forma del mismo determinante sería propiamente equivalente a una y sólo una de ellas (al contrario otras serían propiamente equivalentes entre sí). De donde, resulta claro que *todas las formas del mismo determinante pueden distribuirse en tantas clases como formas permanezcan*, a saber, se ponen en la misma clase todas las formas propiamente equivalentes a una forma reducida. Así para $D = 85$, permanecen las formas

$$(1, 0, 85), \quad (2, 1, 43), \quad (5, 0, 17), \quad (10, 5, 11)$$
$$(-1, 0, -85), \quad (-2, 1, -43), \quad (-5, 0, -17), \quad (-10, 5, -11).$$

Por lo que, todas las formas del determinante -85 podrán distribuirse en ocho clases según sean propiamente equivalentes o a la primera forma, o a la segunda etc. Desde luego, es claro que las formas colocadas en la misma clase serán propiamente equivalentes, y las formas de diferentes clases no pueden ser propiamente equivalentes. Pero más adelante desarrollaremos con mucho detalle este argumento concerniente a la clasificación de las formas. Aquí añadimos una sola observación. Mostramos antes que si el determinante de la forma (a, b, c) en negativo $= -D$, entonces a y c tendrán el mismo signo (porque $ac = b^2 + D$, y por lo tanto es positivo). Por la misma razón se percibe fácilmente que, si las formas (a, b, c) y (a', b', c') son equivalentes, todos los a, c, a', c' tendrán el mismo signo. De hecho, si la primera se transforma en la segunda por la sustitución $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, será $a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = a'$, de esto $aa' = (a\alpha + b\beta)^2 + D\gamma^2$ y por tanto ciertamente es no negativo. Puesto que ni a ni a' puede ser $= 0$, aa' será positivo y por eso los signos de a y a' serán los mismos. De esto es claro que las formas cuyos términos extremos son positivos están completamente separadas de aquéllas cuyos términos extremos son negativos. Sólo basta considerar estas formas reducidas, las que tienen sus términos extremos positivos; puesto que las restantes son iguales en número y provienen de ellas al asignar signos opuestos a los términos extremos. Lo mismo vale para las formas rechazadas o retenidas de las reducidas.

176.

Tenemos aquí una tabla de formas para ciertos determinantes negativos, según las cuales todas las restantes del mismo determinante pueden separarse en clases. Según la observación del artículo anterior, listamos únicamente la mitad, a saber,

aquéllas cuyos términos extremos son positivos.

D	
1	$(1,0,1)$.
2	$(1,0,2)$.
3	$(1,0,3)$, $(2,1,2)$.
4	$(1,0,4)$, $(2,0,2)$.
5	$(1,0,5)$, $(2,1,3)$.
6	$(1,0,6)$, $(2,0,3)$.
7	$(1,0,7)$, $(2,1,4)$.
8	$(1,0,8)$, $(2,0,4)$, $(3,1,3)$.
9	$(1,0,9)$, $(2,1,5)$, $(3,0,3)$.
10	$(1,0,10)$, $(2,0,5)$.
11	$(1,0,11)$, $(2,1,6)$, $(3,1,4)$, $(3,-1,4)$.
12	$(1,0,12)$, $(2,0,6)$, $(3,0,4)$, $(4,2,4)$.

Sería superfluo continuar esta tabla, dado que enseñaremos luego un método mucho más adecuado para construirla.

Es evidente que cada forma del determinante -1 es propiamente equivalente a la forma x^2+y^2 si sus términos extremos son positivos, pero equivalente a $-x^2-y^2$ si son negativos. Cada forma del determinante -2 cuyos términos son positivos es equivalente a la forma x^2+2y^2, etc. Cada forma del determinante -11 cuyos términos extremos son positivos es equivalente a una de éstas x^2+11y^2, $2x^2+2xy+6y^2$, $3x^2+2xy+4y^2$, $3x^2-2xy+4y^2$, etc.

177.

Problema. *Se tiene una serie de formas de las cuales cada una es contigua a la parte posterior de la precedente y se desea una transformación propia de la primera en cualquier forma de la serie.*

Solución. Sean las formas $(a,b,a')=F$; $(a',b',a'')=F'$; $(a'',b'',a''')=F''$; $(a''',b''',a'''')=F'''$ etc. Se denotan $\frac{b+b'}{a'}$, $\frac{b'+b''}{a''}$, $\frac{b''+b'''}{a'''}$ etc., respectivamente por h', h'', h''' etc. Sean x, y; x', y'; x'', y'' etc., las indeterminadas de las formas F, F', F''

etc. Se supone que F se transmuta

$$\begin{aligned} &\text{en } F' \text{ poniendo } x = \alpha' x' + \beta' y', \qquad y = \gamma' x' + \delta' y' \\ &F'' \ . \ . \ . \ . \ x = \alpha'' x'' + \beta'' y'', \qquad y = \gamma'' x'' + \delta'' y'' \\ &F''' \ . \ . \ . \ . \ x = \alpha''' x''' + \beta''' y''', \quad y = \gamma''' x''' + \delta''' y''' \end{aligned}$$

etc.

Entonces, puesto que F se transforma en F' poniendo $x = -y', \quad y = x' + h' y'$
F' en F'' poniendo $x' = -y'', \ y' = x'' + h'' y''$
F'' en F''' poniendo $x'' = -y''', \ y'' = x''' + h''' y'''$
etc. (art. 160)

fácilmente se encuentra el algoritmo siguiente (art. 159):

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h' \\ \alpha'' = \beta' & \beta'' = h''\beta' - \alpha' & \gamma'' = \delta' & \delta'' = h''\delta' - \gamma' \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \alpha'' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \gamma'' \\ \alpha'''' = \beta''' & \beta'''' = h''''\beta''' - \alpha''' & \gamma'''' = \delta''' & \delta'''' = h''''\delta''' - \gamma''' \end{array}$$

etc.,

o sea

$$\begin{array}{llll} \alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h' \\ \alpha'' = \beta' & \beta'' = h''\beta' & \gamma'' = \delta' & \delta'' = h''\delta' - 1 \\ \alpha''' = \beta'' & \beta''' = h'''\beta'' - \beta' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \delta' \\ \alpha'''' = \beta''' & \beta'''' = h''''\beta''' - \beta'' & \gamma'''' = \delta''' & \delta'''' = h''''\delta''' - \delta'' \end{array}$$

etc.

Puede deducirse sin dificultad tanto de su formación como del art. 159 que todas estas transformaciones son propias.

Este algoritmo bien simple y preparado para los cálculos es análogo al algoritmo expuesto en el artículo 27, al cual también puede reducirse*). Además, esta solución no está restringida a las formas de un determinante negativo, si no a todos los casos donde ninguno de los números a', a'', a''', etc., $= 0$.

*) Será, en la notación del art. 27

$$\beta^n = \pm[-h'', h''', -h'''', \ldots \pm h^n]$$

donde los signos ambiguos puestos deben ser $--$; $-+$; $+-$; $++$ conforme a que n sea de la forma

178.

PROBLEMA. *Dadas dos formas propiamente equivalentes a F y f del mismo determinante negativo, encontrar alguna transformación propia de la una en la otra.*

Solución. Supongamos que la forma F es (A, B, A'), y que por el método del artículo 171 se ha encontrado la progresión de formas (A', B', A'') y (A'', B'', A''') etc. hasta la forma reducida (A^m, B^m, A^{m+1}). De manera similar supongamos que f es (a, b, a') y que por el mismo método se encuentra la serie (a', b', a'') y (a'', b'', a''') hasta la forma reducida (a^n, b^n, a^{n+1}). Entonces pueden tener lugar dos casos.

I. Si las formas (A^m, B^m, A^{m+1}) y (a^n, b^n, a^{n+1}) o son idénticas u opuestas y, a la vez, ambiguas, entonces, las formas (A^{m-1}, B^{m-1}, A^m) y $(a^n, -b^{n-1}, a^{n-1})$ serán contiguas (donde A^{m-1} denota el penúltimo término de la progresión A, A', A'', $\ldots A^m$, y de manera semejante B^{m-1}, a^{n-1}, b^{n-1}). Puesto que $A^m = a^n$, $B^{m-1} \equiv -B^m \pmod{A^m}$, $b^{n-1} \equiv -b^n \pmod{a^n \text{ o sea } A^m}$, resulta $B^{m-1} - b^{n-1} \equiv b^n - B^m$ y, por tanto $\equiv 0$, si las formas (A^m, B^m, A^{m+1}), (a^n, b^n, a^{n+1}) son idénticas, y $\equiv 2b^n$ y por tanto $\equiv 0$, si son opuestas y ambiguas. Por lo que, en las progresiones de las formas

$$\begin{gathered}(A, B, A'), \quad (A', B', A''), \quad \ldots (A^{m-1}, B^{m-1}, A^m), \\ (a^n, -b^{n-1}, a^{n-1}), \quad (a^{n-1}, -b^{n-2}, a^{n-2}), \quad \ldots (a', -b, a), \quad (a, b, a')\end{gathered}$$

cada forma será contigua a la precedente; y de esto, por el artículo anterior podrá encontrarse una transformación propia de la primera F en la segunda f.

II. Si las formas (A^m, B^m, A^{m+1}) y (a^n, b^n, a^{n+1}) no son idénticas, sino opuestas y, a la vez, $A^m = A^{m+1} = a^n = a^{n+1}$; entonces, la progresión de las formas

$$\begin{gathered}(A, B, A'), \quad (A', B', A''), \quad \ldots (A^m, B^m, A^{m+1}), \\ (a^n, -b^{n-1}, a^{n-1}), \quad (a^{n-1}, -b^{n-2}, a^{n-2}), \quad \ldots (a', -b, a), \quad (a, b, a')\end{gathered}$$

estarán provistas de la misma propiedad. Puesto que $A^{m+1} = a^n$, y $B^m - b^{n-1} = -(b^n + b^{n-1})$ será divisible por a^n. De donde, por el artículo anterior, se encontrará una transformación propia de la primera forma F en la segunda f.

$4k + 0$; 1; 2; 3; y

$$\delta^n = \pm[h', -h'', h''', \ldots \pm h^n]$$

donde los signos ambiguos deben ser $+-$; $++$; $--$; $-+$, según n sea de la forma $4k + 0$; 1; 2; 3. Pero dado que esto puede confirmarse fácilmente por sí mismo, la brevedad no permite exponerlo con amplitud.

Ejemplo. Para las formas $(23, 38, 63)$ y $(15, 20, 27)$ se tiene la progresión $(23, 38, 63)$, $(63, 25, 10)$, $(10, 5, 3)$, $(3, 1, 2)$, $(2, -7, 27)$, $(27, -20, 15)$, $(15, 20, 27)$ por lo cual

$$h' = 1, \quad h'' = 3, \quad h''' = 2, \quad h'''' = -3, \quad h''''' = -1, \quad h'''''' = 0$$

De esto se deduce que la transformación de la forma $23x^2 + 76xy + 63y^2$ en $15t^2 + 40tu + 27u^2$ es ésta: $x = -13t - 18u$, $y = 8t + 11u$.

De esta solución, se deduce sin dificultad la solución del problema: *Si las formas F y f son impropiamente equivalentes, hallar una transformación impropia de la forma F en f.* De hecho, sea $f = at^2 + 2btu + a'u^2$, entonces la forma opuesta $ap^2 - 2bpq + a'q^2$ será propiamente equivalente a la forma F. Búsquese una transformación propia de la forma F en $x = \alpha p + \beta q$ y $y = \gamma p + \delta q$, entonces es claro que F se transforma en f dadas $x = \alpha t - \beta u$, $y = \gamma t - \delta u$; por lo que esta transformación será impropia.

Si, por lo tanto, las formas F y f son equivalentes tanto propia como impropiamente, entonces podrá encontrarse tanto una transformación propia como una impropia.

179.

PROBLEMA. *Si las formas F y f son equivalentes, hallar todas las transformaciones de la forma F en f.*

Solución. Si las formas F y f son equivalentes de una sola manera, i.e., solamente propiamente o solamente impropiamente, por el artículo precedente búsquese alguna transformación de la forma F en f. Es claro que no pueden darse otras más que aquéllas semejantes a ésta. Si, por otro lado las formas F y f son equivalentes tanto propia como impropiamente, búsquense dos transformaciones: la una propia y la otra impropia. Sea la forma $F = (A, B, C)$, $B^2 - AC = -D$, y el máximo común divisor de los números A, $2B$, $C = m$. Entonces es claro del artículo 162 que, en el primer caso, todas las transformaciones de la forma F en f pueden deducirse de una transformación; y en el segundo, todas las propias de una propia y todas las impropias de una impropia, si se tuvieran todas las soluciones de la ecuación $t^2 + Du^2 = m^2$. Por lo tanto, encontradas éstas, el problema se habría resuelto.

Se tiene, sin embargo, $D = AC - B^2$, $4D = 4AC - 4B^2$; por lo cual $\frac{4D}{m^2} = 4(\frac{AC}{m^2}) - (\frac{2B}{m})^2$ será un entero. Ahora, si

1) $\frac{4D}{m^2} > 4$, será $D > m^2$; de donde en $t^2 + Du^2 = m^2$, u deberá ser $= 0$, y por tanto t no puede tener otros valores más que $+m$ y $-m$. De esto, si F y f son equivalentes de una sola manera, entonces no puede darse alguna transformación más que

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

la cual resulta poniendo $t = m$ (artículo 162), y otra

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y'.$$

Si por el otro lado F y f son equivalentes tanto propia como impropiamente, y si se tiene alguna transformación propia

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

y una impropia

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'$$

entonces no se presentará otra transformación propia salvo aquéllas (poniendo $t = m$) y éstas

$$x = -\alpha x' - \beta y', \quad y = -\gamma x' - \delta y'$$

(poniendo $t = -m$) y de modo semejante ninguna impropia salvo

$$x = \alpha' x' + \beta' y', \quad y = \gamma' x' + \delta' y'; \quad y \quad x = -\alpha' x' - \beta' y', \quad y = -\gamma' x' - \delta' y'.$$

2) Si $\frac{4D}{m^2} = 4$, o sea $D = m^2$, la ecuación $t^2 + Du^2 = m^2$ admitirá cuatro soluciones: t, $u = m$, 0; $-m$, 0; 0, 1; 0, -1. De esto, si F y f son equivalentes de una sola manera y si tenemos alguna transformación

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

resultarán *cuatro* ecuaciones:

$$x = \pm\alpha x' \pm \beta y', \quad y = \pm\gamma x' \pm \delta y'$$
$$x = \mp\frac{\alpha B + \gamma C}{m} x' \mp \frac{\beta B + \delta C}{m} y', \quad y = \pm\frac{\alpha A + \gamma B}{m} x' \pm \frac{\beta A + \delta B}{m} y'$$

Por otro lado, si F y f son equivalentes de dos maneras, o sea, si además de esta transformación dada se tiene otra no semejante a esta misma, ella también

proporcionará cuatro no semejantes a ella de tal manera que se tengan *ocho* transformaciones. Además, en este caso puede demostrarse que F y f siempre son equivalentes de dos maneras. Como $D = m^2 = AC - B^2$, m también dividirá a B. El determinante de la forma $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ será $= -1$, por lo que será equivalente a la forma $(1, 0, 1)$ o a $(-1, 0, -1)$. Sin embargo, se percibe que, mediante la misma transformación por la cual se transforma $(\frac{A}{m}, \frac{B}{m}, \frac{C}{m})$ en $(\pm 1, 0, \pm 1)$, se transformará la forma (A, B, C) en una ambigua $(\pm m, 0, \pm m)$. Por lo que, la forma (A, B, C), equivalente a una ambigua, equivaldrá tanto propia como impropiamente a cualquier forma a la cual sea equivalente.

3) Si $\frac{4D}{m^2} = 3$, o sea $4D = 3m^2$, entonces m será par y el total de soluciones de la ecuación $t^2 + Du^2 = m^2$ será seis:

$$t,\, u \quad = m,\, 0; \quad -m,\, 0; \quad \frac{1}{2}m,\, 1; \quad \frac{-1}{2}m,\, -1; \quad \frac{1}{2}m,\, -1; \quad \frac{-1}{2}m,\, 1.$$

Por consiguiente, si se tienen dos transformaciones no semejantes de la forma F en f,

$$\begin{array}{ll} x = \alpha x' + \beta y' & y \,=\, \gamma x' + \delta y' \\ x = \alpha' x' + \beta' y' & y = \gamma' x' + \delta' y' \end{array}$$

se tendrán doce transformaciones, a saber, seis semejantes a la primera

$$\begin{array}{l} x = \pm\alpha x' \pm \beta y', \quad y = \pm\gamma x' \pm \delta y' \\ x = \pm(\frac{1}{2}\alpha - \frac{\alpha B + \gamma C}{m})x' \pm (\frac{1}{2}\beta - \frac{\beta B + \delta C}{m})y' \\ y = \pm(\frac{1}{2}\gamma + \frac{\alpha A + \gamma B}{m})x' \pm (\frac{1}{2}\delta + \frac{\beta A + \delta B}{m})y' \\ x = \pm(\frac{1}{2}\alpha + \frac{\alpha B + \gamma C}{m})x' \pm (\frac{1}{2}\beta + \frac{\beta B + \delta C}{m})y' \\ y = \pm(\frac{1}{2}\gamma - \frac{\alpha A + \gamma B}{m})x' \pm (\frac{1}{2}\delta - \frac{\beta A + \delta B}{m})y' \end{array}$$

y seis semejantes a la segunda, que se originan de éstas al sustituir α, β, γ, δ por α', β', γ', δ'.

Para demostrar que en este caso F y f siempre son equivalentes de ambas maneras, consideremos lo siguiente. El determinante de la forma $(\frac{2A}{m}, \frac{2B}{m}, \frac{2C}{m})$ será $= \frac{-4D}{m^2} = -3$, y por tanto esta forma es equivalente (art. 176) o a la forma $(\pm 1, 0, \pm 3)$, o a la forma $(\pm 2, \pm 1, \pm 2)$. De donde se sabe que la forma (A, B, C) es equivalente

o a la forma $(\pm\frac{1}{2}m, 0, \pm\frac{3}{2}m)$ o a la forma $(\pm m, \frac{1}{2}m, \pm m)$*), las cuales son ambas ambiguas, y, por tanto, de ambas maneras equivalente a una de ellas.

4) Si se supone $\frac{4D}{m^2} = 2$, sería $(\frac{2B}{m})^2 = 4\frac{AC}{m^2} - 2$, y, por tanto, $\equiv 2 \pmod 4$. Pero, como ningún cuadrado puede ser $\equiv 2 \pmod 4$, este caso no puede darse aquí.

5) Suponiendo que $\frac{4D}{m^2} = 1$, sería $(\frac{2B}{m})^2 = 4\frac{AC}{m^2} - 1 \equiv -1 \pmod 4$. Pero como esto es imposible, este caso tampoco puede ocurrir aquí.

Además, como D no puede ser ni $= 0$ ni negativo, no pueden darse otros casos diferentes más que los enumerados.

180.

PROBLEMA. *Hallar todas las representaciones del número dado M por la forma $ax^2 + 2bxy + cy^2 \ldots F$, del determinante negativo $-D$, en la cual x e y tengan valores primos entre sí.*

Solución. Por el artículo 154, notamos que M no puede representarse tal como se necesita, a menos que $-D$ sea residuo cuadrático de M. Así, primero búsquense todos los valores diferentes (i.e. incongruentes) de la expresión $\sqrt{-D} \pmod M$; sean estos valores $N, -N, N', -N', N'', -N''$ etc. Para simplificar los cálculos, se pueden determinar todos los N, N', etc., de tal manera que no sean $> \frac{1}{2}M$. Puesto que cualquier representación debe pertenecer a alguno de estos valores, consideraremos cada uno separadamente.

Si las formas F, $(M, N, \frac{D+N^2}{M})$ no son propiamente equivalentes, no puede existir ninguna representación de M perteneciente al valor N (artículo 168). Si al contrario existen, buscaremos una transformación propia de la forma F en

$$Mx'^2 + 2Nx'y' + \frac{D+N^2}{M}y'^2$$

la cual sea

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

y $x = \alpha$, $y = \gamma$ será una representación del número M por F perteneciente al valor N. Sea el máximo común divisor de los números A, $2B$, $C = m$, entonces distinguiremos tres casos (artículo anterior):

*) Puede demostrarse que la forma (A, B, C) necesariamente equivaldrá a la segunda; pero esto no es necesario aquí.

1) Si $\frac{4D}{m^2} > 4$ no se darán representaciones pertenecientes a N salvo estas *dos* $x = \alpha$, $y = \gamma$ y $x = -\alpha$, $y = -\gamma$ (artículos 169 y 179).

2) Si $\frac{4D}{m^2} = 4$ se tendrán *cuatro* representaciones

$$x = \pm\alpha, \quad y = \pm\gamma; \qquad x = \mp\frac{\alpha B + \gamma C}{m}, \quad y = \pm\frac{\alpha A + \gamma B}{m}$$

3) Si $\frac{4D}{m^2} = 3$ se tendrán *seis* representaciones

$$\begin{array}{ll} x = \pm\alpha & y = \pm\gamma \\ x = \pm(\frac{1}{2}\alpha - \frac{\alpha B+\gamma C}{m}) & y = \pm(\frac{1}{2}\gamma + \frac{\alpha A+\gamma B}{m}) \\ x = \pm(\frac{1}{2}\alpha + \frac{\alpha B+\gamma C}{m}) & y = \pm(\frac{1}{2}\gamma - \frac{\alpha A+\gamma B}{m}) \end{array}$$

De la misma manera se deben buscar las representaciones pertenecientes a los valores $-N$, N', $-N'$ etc.

181.

La investigación de las representaciones del número M por la forma F, en la cual x e y tienen valores no primos entre sí, puede reducirse fácilmente al caso ya considerado. Suponga que se hace tal representación al poner $x = \mu e$ e $y = \mu f$ de manera que μ sea el máximo común divisor de μe y μf, o sea, e y f son primos entre sí. Entonces tendremos que $M = \mu^2(Ae^2 + 2Bef + Cf^2)$ y, por lo tanto, será divisible por μ^2. Sin embargo, la sustitución $x = e$, $y = f$ será una representación del número $\frac{M}{\mu^2}$ por la forma F, en la cual x e y tienen valores primos entre sí. Si M no es divisible por ningún cuadrado (salvo 1), por ejemplo, si es un número primo, no se darán tales representaciones de M. Sin embargo, si M involucra divisores cuadrados, sean éstas μ^2, ν^2, π^2 etc. Se buscan primero todas las representaciones del número $\frac{M}{\mu^2}$ por la forma (A, B, C), en las cuales x e y tienen valores primos entre sí. Tales valores, si se multiplican por μ, suministrarán todas las representaciones de M en las cuales el máximo común divisor de los números x e y es μ. De modo semejante, todas las representaciones de $\frac{M}{\nu^2}$, en las cuales los valores de x e y son primos entre sí, producirán todas las representaciones de M en las que el máximo común divisor de los valores x e y es ν etc.

Por lo tanto, es claro que por las reglas precedentes pueden encontrarse todas las representaciones de un número dado por una forma dada de un determinante negativo.

Aplicaciones especiales a la descomposición de los números en dos cuadrados, en un cuadrado simple y uno doble, en un cuadrado simple y uno triple .

182.

Pasamos a ciertos casos especiales tanto por su elegancia notable como por el incesante trabajo empleado en ellos por el ilustre Euler, por lo que están provistos de una belleza casi clásica.

I. Ningún número puede representarse por la forma $x^2 + y^2$, de modo que x sea primo a y (o sea descompuesto en dos cuadrados primos entre sí) a no ser que -1 sea un residuo cuadrático de él. Sin embargo, tales números tomados positivamente sí pueden serlo. Sea M un número tal, y todos los valores de la expresión $\sqrt{-1} \pmod{M}$ éstos: N, $-N$, N', $-N'$, N'', $-N''$ etc., entonces, por el artículo 176 la forma $(M, N, \frac{N^2+1}{M})$ será propiamente equivalente a la forma $(1, 0, 1)$. Sea $x = \alpha y' + \beta y'$, $y = \gamma x' + \delta y'$ una transformación propia de la segunda en la primera, y las representaciones del número M por la forma $x^2 + y^2$ pertenecientes a N estas cuatro*): $x = \pm\alpha$, $y = \pm\gamma$; $x = \mp\gamma$, $y = \pm\alpha$.

Puesto que la forma $(1, 0, 1)$ es ambigua, de hecho será propiamente equivalente a la forma $(M, -N, \frac{N^2+1}{M})$, y por ende aquélla se transmutará en ésta, poniendo $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$. De esto se derivan cuatro representaciones de M pertenecientes a $-N$, $x = \pm\alpha$, $y = \mp\gamma$; $x = \pm\gamma$, $y = \pm\alpha$. Así pues, existen ocho representaciones de M, la mitad de los cuales pertenece a N, la otra mitad a $-N$; pero todas éstas representan sólo *una* descomposición del número M en dos cuadrados, $M = \alpha^2 + \gamma^2$, si sólo consideramos a los cuadrados mismos, pero no al orden de las raíces ni a sus signos.

Por tanto, si no existen otros valores de la expresión $\sqrt{-1} \pmod{M}$, salvo N y $-N$, lo cual e.g. resulta cuando M es un número primo, M podrá resolverse en dos cuadrados primos entre sí de una sola manera. Puesto que -1 es un residuo cuadrático de cualquier número primo de la forma $4n + 1$ (art. 108), entonces es evidente que un número primo no puede descomponerse en dos cuadrados no primos entre sí. Así tendremos el teorema:

Cualquier número primo de la forma $4n + 1$ *puede descomponerse como suma de dos cuadrados, y de una sola manera.*

$$1 = 0 + 1, \quad 5 = 1 + 4, \quad 13 = 4 + 9, \quad 17 = 1 + 16, \quad 29 = 4 + 25, \quad 37 = 1 + 36,$$

*) Es claro que este caso está contenido en (2) del artículo 180.

$$41 = 16 + 25, \quad 53 = 4 + 49, \quad 61 = 25 + 36, \quad 73 = 9 + 64, \quad 89 = 25 + 64,$$
$$97 = 16 + 81 \text{ etc.}$$

Este teorema elegantísimo ya fue conocido por Fermat, pero fue demostrado primero por el ilustre Euler, *Comm. nov. Petr.*, V, 1754 y 1755, p. 3. En el cuarto volumen existe una disertación perteneciente al mismo argumento (p. 3) pero entonces aún no había encontrado una solución completa, véase especialmente artículo 27.

Por lo tanto, si algún número de la forma $4n + 1$ puede resolverse en dos cuadrados o bien en varias maneras, o bien de ninguna manera, entonces no será primo.

Al contrario, si la expresión $\sqrt{-1}$ (mod. M) tiene otros valores, además de N y $-N$, se presentarán todavía otras representaciones de M, pertenecientes a éstos. Así pues, en este caso M podrá resolverse de varias maneras en dos cuadrados; e.g. $65 = 1 + 64 = 16 + 49$, $221 = 25 + 196 = 100 + 121$.

Las restantes representaciones, en las cuales x e y tienen valores no primos entre sí, pueden encontrarse con facilidad por nuestro método general. Sólo observamos que, si algún número que involucra factores de la forma $4n + 3$ no puede liberarse de éstos por ninguna división por un cuadrado (esto sucederá si uno o varios de tales factores tienen *un exponente impar*), entonces dicho número tampoco puede resolverse de manera alguna en dos cuadrados*).

II. Ningún número del cual -2 es un no residuo podrá representarse por la forma $x^2 + 2y^2$, de tal modo que x sea primo a y, pero todos los restantes sí podrán. Sea -2 un residuo del número M, y N algún valor de la expresión $\sqrt{-2}$ (mod. M). Entonces, por art. 176 las formas $(1,\ 0,\ 2)$ y $(M, N, \frac{N^2+2}{M})$ serán propiamente equivalentes. La primera se transforma en la segunda poniendo $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, y $x = \alpha$, $y = \gamma$ será una representación del número M perteneciente a

*) Si el número $M = 2^\mu S a^\alpha b^\beta c^\gamma \ldots$ de manera que a, b, c sean números primos diferentes de la forma $4n + 1$ y si S es el producto de todos los factores primos de M de la forma $4n + 3$ (a tal forma cualquier número positivo puede reducirse, haciendo $\mu = 0$ cuando M es impar, y $S = 1$, cuando M no involucra factores de la forma $4n + 3$), entonces M *de ninguna manera* podrá resolverse en dos cuadrados si S no es un cuadrado, pero si S es un cuadrado, se presentarán $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1)$ etc. descomposiciones de M cuando alguno de los números α, β, γ, etc. es impar, pero $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1)$ etc. $+ \frac{1}{2}$ cuando todos α, β, γ, etc. son pares (puesto que se examinan solamente los cuadrados). Los que son versados en el cálculo de combinaciones podrán llevar a cabo la demostración de este teorema (en el que, como para otros *casos particulares*, no podemos detenernos) sin dificultad a partir de nuestra teoría general. Vea artículo 105.

N. Además de ésta, tendremos $x = -\alpha$ e $y = -\gamma$, y no existen otras pertenecientes a N (artículo 180).

De modo semejante, se percibe que las representaciones $x = \pm\alpha$, $y = \mp\gamma$ pertenecen al valor $-N$. Sin embargo estas cuatro representaciones presentan únicamente una descomposición de M en un cuadrado y el doble de un cuadrado, y si más allá de N y $-N$ no se dan otros valores de la expresión $\sqrt{-2}$ (mod. M), tampoco existirán otras descomposiciones. De esto, con la ayuda de las proposiciones del artículo 116, se deduce fácilmente este teorema:

Cualquier número primo de la forma $8n+1$ *u* $8n+3$ *puede descomponerse en un cuadrado y un cuadrado duplicado de una sola manera.*

$$1 = 1 + 0, \quad 3 = 1 + 2, \quad 11 = 9 + 2, \quad 17 = 9 + 8, \quad 19 = 1 + 18, \quad 41 = 9 + 32,$$
$$43 = 25 + 18, \quad 59 = 9 + 50, \quad 67 = 49 + 18, \quad 73 = 1 + 72, \quad 83 = 81 + 2,$$
$$89 = 81 + 8, \quad 97 = 25 + 72 \quad \text{etc.}$$

Fermat también conocía este teorema, como varios semejantes; pero el ilustre Lagrange dio la primera demostración, *Suite des recherches d'Arithmétique,* Nouv. Mém. de l'Ac. de Berlín, 1775, p. 323. Ya el ilustre Euler había llevado a cabo mucho con relación al mismo argumento, *Specimen de usu observationum in mathesi pura,* Comm. nov. Petr., VI, p. 185. Pero nunca encontró una demostración completa del teorema. Compárese también la disertación en el Tomo VIII (para los años 1760 y 1761) *Supplementum quorundam theorematum arithmeticorum*, al final.

III. Se demuestra por un método semejante que, cada número del cual -3 es un residuo cuadrático, puede representarse o por la forma $x^2 + 3y^2$ o por $2x^2 + 2xy + 2y^2$, de manera que el valor de x sea primo al valor de y. Por lo tanto, puesto que -3 es un residuo de todos los números primos de la forma $3n+1$ (art. 119), y ya que únicamente números *pares* pueden representarse por la forma $2x^2+2xy+2y^2$. Tal como arriba se tiene este teorema:

Cualquier número primo de la forma $3n+1$ *puede descomponerse como suma de un cuadrado y un cuadrado triplicado y sólo de una manera.*

$$1 = 1 + 0, \quad 7 = 4 + 3, \quad 13 = 1 + 12, \quad 19 = 16 + 3, \quad 31 = 4 + 27, \quad 37 = 25 + 12,$$
$$43 = 16 + 27, \quad 61 = 49 + 12, \quad 67 = 64 + 3, \quad 73 = 25 + 48 \quad \text{etc.}$$

El ilustre Euler presentó la primera demostración de este teorema en el comentario citado, *Comm. nov. Petr.,* VIII, p. 105.

De modo semejante podremos adelantar y mostrar que todo número primo de la forma $20n+1$, o $20n+3$, o $20n+7$, o $20n+9$ (de los cuales -5 es un residuo) puede representarse por una de las dos formas x^2+5y^2, $2x^2+2xy+3y^2$, y los números primos de la forma $20n+1$ y $20n+9$ pueden representarse por la primera forma, los números primos de la forma $20n+3$, $20n+7$ por la segunda, y además los dobles de los primos de la forma $20n+1$, $20n+9$ por la forma $2x^2+2xy+3y^2$ y los dobles de los primos de la forma $20n+3$, $20n+7$ por la forma x^2+5y^2. Pero esta proposición y otras infinitas particulares podrán derivarse de las precedentes y de lo que se discuta más adelante. Pasamos ahora a las *formas de un determinante positivo.* Dado que la naturaleza de ellas es completamente diferente cuando el determinante es un cuadrado que cuando no es un cuadrado, excluiremos primero las formas de un determinante cuadrado y luego las consideraremos por separado.

Sobre las formas de un determinante positivo no cuadrado.

183.

PROBLEMA. *Dada cualquier forma (a, b, a'), cuyo determinante positivo y no cuadrado es $= D$, se debe encontrar una forma (A, B, C) propiamente equivalente a ella, en la cual B sea positivo y $< \sqrt{D}$ y donde A, si es positivo o $-A$, si A es negativo, estará situada entre $\sqrt{D} + B$ y $\sqrt{D} - B$.*

Resolución. Suponemos que en la forma propuesta las dos condiciones aún no tienen lugar; de lo contrario no sería necesario buscar otra forma. Además, observamos que en una forma de un determinante *no cuadrado*, el primer término o el último no puede ser $= 0$ (artículo 171, nota de pie). Sea $b' \equiv -b \pmod{a'}$ de modo que esté situado entre los límites $\sqrt{D}$ y $\sqrt{D} \mp a'$ (tomando el signo superior cuando a' es positivo, el inferior cuando es negativo), lo cual es posible por un razonamiento como el del art. 3. Sea $\frac{b'^2-D}{a'} = a''$, que será un entero ya que $b'^2 - D \equiv b^2 - D \equiv aa' \equiv 0 \pmod{a'}$. Ahora, si $a'' < a'$, se tomará $b'' \equiv -b' \pmod{a''}$ y situado entre $\sqrt{D}$ y $\sqrt{D} \mp a''$ (según a'' sea positivo o negativo) y $\frac{b''^2-D}{a''} = a'''$. Si de nuevo $a''' < a''$, sea otra vez $b''' \equiv -b'' \pmod{a'''}$ y situado entre $\sqrt{D}$ y $\sqrt{D} \mp a'''$ y $\frac{b'''^2-D}{a'''} = a''''$. Se continuará este procedimiento para formar la progresión a', a'', a''', a'''' etc. hasta un término a^{m+1} no menor que el precedente a^m. Esto finalmente debe suceder, pues de lo contrario se tendrá una progresión infinita de números enteros continuamente decrecientes. Entonces, dadas $a^m = A$, $b^m = B$ y $a^{m+1} = C$, la forma (A, B, C) satisfará todas las condiciones.

Demostración. I. Puesto que en la progresión de formas (a, b, a'), (a', b', a''), (a'', b'', a''') etc. cualquiera es contigua a la precedente, la última (A, B, C) será propiamente equivalente a la primera (a, b, a').

II. Puesto que B está situado entre $\sqrt{D}$ y $\sqrt{D} \mp A$ (tomando siempre el signo superior cuando A es positivo, el inferior cuando A es negativo), es claro que, si se pone $\sqrt{D} - B = p$, $B - (\sqrt{D} \mp A) = q$, estos p y q serán positivos. Se confirma fácilmente que $q^2 + 2pq + 2p\sqrt{D} = D + A^2 - B^2$; por lo que $D + A^2 - B^2$ será un número positivo, el cual pondremos $= r$. De esto, puesto que $D = B^2 - AC$ resulta $r = A^2 - AC$ y por tanto $A^2 - AC$ será un número positivo. Pero, ya que por hipótesis A no es mayor que C, es claro que esto no puede suceder a menos que AC sea negativo, y por lo tanto los signos de A y C deben ser opuestos. De esto, $B^2 = D + AC < D$ y por tanto $B < \sqrt{D}$.

III. Además, ya que $-AC = D - B^2$, tendremos $AC < D$, y de esto (puesto que A no es $> C$) $A < \sqrt{D}$. Por lo que, $\sqrt{D} \mp A$ será positivo, y por tanto también lo será B, el cual está situado entre los límites $\sqrt{D}$ y $\sqrt{D} \mp A$.

IV. De esto, con más razón $\sqrt{D} + B \mp A$ es positivo, y dado que $\sqrt{D} - B \mp A = -q$, es negativo, $\pm A$ estará situado entre $\sqrt{D} + B$ y $\sqrt{D} - B$. *Q. E. D.*

Ejemplo. Propuesta la forma $(67, 97, 140)$ cuyo determinante es $= 29$, se encontrará aquí la progresión de las formas $(67, 97, 140)$, $(140, -97, 67)$, $(67, -37, 20)$, $(20, -3, -1)$ y $(-1, 5, 4)$. La última es la buscada.

Llamaremos *formas reducidas* a tales formas (A, B, C) de un determinante positivo no cuadrado D, en las cuales A, tomado positivamente, está situado entre $\sqrt{D} + B$ y $\sqrt{D} - B$, siendo B positivo y $< \sqrt{D}$. Así pues las formas reducidas de un determinante positivo no cuadrado difieren de las formas reducidas de un determinante negativo. Pero debido a la gran analogía entre éstas y aquéllas, no quisimos introducir diferentes denominaciones.

184.

Si se pudiera reconocer la equivalencia de dos formas *reducidas* de determinante positivo con la misma facilidad que en el caso de aquéllas de determinante negativo (art. 172) se reconocería sin dificultad la equivalencia de dos formas *cualesquiera* de determinante positivo. Pero aquí el asunto es muy diferente, y puede suceder que muchas formas reducidas sean equivalentes entre sí. Antes de dedicarnos a este problema, será necesario inquirir más detalladamente en la naturaleza de las

formas reducidas (de un determinante positivo no cuadrado, lo cual siempre está supuesto).

1) Si (a, b, c) es una forma reducida, a y c tendrán signos opuestos. Ya que puesto el determinante de la forma $= D$, será $ac = b^2 - D$, y por lo tanto, puesto que $b < \sqrt{D}$, será negativo.

2) El número c tomado positivamente estará situado, tal como a, entre $\sqrt{D}+b$ y $\sqrt{D} - b$. Puesto que $-c = \frac{D-b^2}{a}$; entonces c, abstraído del signo, estará situado entre $\frac{D-b^2}{\sqrt{D}+b}$ y $\frac{D-b^2}{\sqrt{D}-b}$, i.e., entre $\sqrt{D} - b$ y $\sqrt{D} + b$.

3) De esto es evidente que (c, b, a) también será una forma reducida.

4) Tanto a como c serán $< 2\sqrt{D}$. En efecto, ambos son $< \sqrt{D} + b$, y así con más razón $< 2\sqrt{D}$.

5) El número b estará situado entre $\sqrt{D}$ y $\sqrt{D} \mp a$ (tomando el signo superior cuando a es positivo, el inferior cuando es negativo). Puesto que $\pm a$ cae entre $\sqrt{D}+b$ y $\sqrt{D} - b$, entonces $\pm a - (\sqrt{D} - b)$, o sea $b - (\sqrt{D} \mp a)$ será positivo; sin embargo $b - \sqrt{D}$ es negativo, debido a que b estará situado entre $\sqrt{D}$ y $\sqrt{D} \mp a$. Del mismo modo se demuestra que b cae entre $\sqrt{D}$ y $\sqrt{D} \mp c$ (según c sea positivo o negativo).

6) *Cada forma reducida* (a, b, c) *es contigua por una u otra parte a una reducida y no a varias.*

Sea $a' = c$, $b' \equiv -b \pmod{a'}$ tal que esté situado entre $\sqrt{D}$ y $\sqrt{D} \mp a'$*), $c' = \frac{b'^2-D}{a'}$, y la forma (a', b', c') estará contigua a la forma (a, b, c) por su última parte. A la vez, es evidente que si existe alguna forma reducida contigua a la forma (a, b, c) por la última parte, ella misma no puede ser diferente a (a', b', c'). Sin embargo, demostramos que ésta se ha reducido así:

A) Si se pone

$$\sqrt{D} + b \mp a' = p, \qquad \pm a' - (\sqrt{D} - b) = q, \qquad \sqrt{D} - b = r$$

entonces por (2) arriba y la definición de forma reducida, p, q y r serán positivos. Además, póngase

$$b' - (\sqrt{D} \mp a') = q', \qquad \sqrt{D} - b' = r'$$

*) Donde los signos son ambiguos, siempre vale el superior cuando a' es positivo, el inferior cuando a' es negativo.

y q' y r' serán positivos, puesto que b' está situado entre $\sqrt{D}$ y $\sqrt{D} \mp a'$. Finalmente, sea $b + b' = \pm ma'$ entonces m será un entero. Es claro que será $p + q' = b + b'$, y por tanto $b + b'$, o sea $\pm ma'$ es positivo, y por eso también lo es m; de donde resulta que $m - 1$ no será negativo. Además, tenemos

$$r + q' \pm ma' = 2b' \pm a', \qquad \text{o sea} \quad 2b' = r + q' \pm (m-1)a'$$

de donde $2b'$ y b' serán necesariamente positivos. Y puesto que $b' + r' = \sqrt{D}$, tendremos $b' < \sqrt{D}$.

B) Además tenemos

$$r \pm ma' = \sqrt{D} + b', \qquad \text{o sea} \quad r \pm (m-1)a' = \sqrt{D} + b' \mp a'$$

por lo cual $\sqrt{D} + b' \mp a'$ será positivo. Puesto que $\pm a' - (\sqrt{D} - b') = q'$, y por lo tanto positivo, $\pm a'$ estará situado entre $\sqrt{D} + b'$ y $\sqrt{D} - b'$. Por esto, (a', b', c') será una forma reducida.

Del mismo modo se demuestra que si tenemos $'c = a$, $'b \equiv -b \pmod{'c}$ con $'b$ situado entre $\sqrt{D}$ y $\sqrt{D} \pm 'c$, y si $'a = \frac{'b^2 - D}{'c}$, entonces la forma $('a, 'b, 'c)$ será reducida. Evidentemente, esta forma también es contigua a la forma (a, b, c) por la primera parte, y salvo $('a, 'b, 'c)$, otra forma reducida no podrá estar provista de esta propiedad.

Ejemplo. La forma reducida $(-14, 3, 13)$ es contigua por la parte última a la reducida $(5, 11, -14)$ cuyo determinante es $= 191$, y por la parte primera es contigua a $(-22, 9, 5)$.

7) Si la forma reducida (a', b', c') es contigua a la forma reducida (a, b, c) por la parte última, la forma (c', b', a') será contigua por la parte primera a la forma reducida (c, b, a). Si la forma $('a, 'b, 'c)$ es contigua por la parte primera a la reducida (a, b, c), la reducida $('c, 'b, 'a)$ será contigua a la reducida (c, b, a) por la parte última. También las formas $(-'a, 'b, -'c)$, $(-a, b, -c)$, $(-a', b', -c')$ serán reducidas, y la segunda contigua a la primera, la tercera a la segunda por la parte última, o sea la primera a la segunda y la segunda a la tercera por la parte primera. De modo semejante, esto vale para las tres formas $(-c', b', -a')$, $(-c, b, -a)$ y $(-'c, 'b, -'a)$. Esto es tan obvio que no es necesario explicarlo.

185.

El número de todas las formas reducidas de un determinante dado D siempre es finito, mas, ellas mismas pueden encontrarse de dos maneras. Denotaremos, de modo indefinido, por (a, b, c) todas las formas reducidas de un determinante D de manera que determinemos todos los valores de a, b, c.

Primer método. Se toma para a todos los números (tanto positiva como negativamente) menores que $2\sqrt{D}$, de los cuales D es un residuo cuadrático, y para cada a en particular se pone b igual a todos los valores positivos de la expresión $\sqrt{D}$ (mod. a) situados entre $\sqrt{D}$ y $\sqrt{D} \mp a$. Pero para cada valor determinado de a y b en particular se pone $c = \frac{b^2 - D}{a}$. Si algunas formas provienen de este modo, en las cuales $\pm a$ está situado afuera de $\sqrt{D} + b$ y $\sqrt{D} - b$, deben rechazarse.

Segundo método. Se toma para b todos los números positivos menores que $\sqrt{D}$, y para cada b en particular se resuelve $b^2 - D$ en dos factores de todas las maneras posibles, los cuales, desechado el signo, estén situados entre $\sqrt{D}+b$ y $\sqrt{D}-b$ y ponemos el uno $= a$, el otro $= c$. Evidentemente cada una de las resoluciones en factores en particular suministrará dos formas; ya que uno u otro factor debe ponerse tanto $= a$, como $= c$.

Ejemplo. Sea $D = 79$, entonces tendremos veintidós valores de a: ∓ 1, 2, 3, 5, 6, 7, 9, 10, 13, 14, 15. De donde se encuentran diecinueve formas:

$$(1, 8, -15), \quad (2, 7, -15), \quad (3, 8, -5), \quad (3, 7, -10), \quad (5, 8, -3), \quad (5, 7, -6),$$
$$(6, 7, -5), \quad (6, 5, -9), \quad (7, 4, -9), \quad (7, 3, -10), \quad (9, 5, -6), \quad (9, 4, -7),$$
$$(10, 7, -3), \quad (10, 3, -7), \quad (13, 1, -6), \quad (14, 3, -5), \quad (15, 8, -1),$$
$$(15, 7, -2), \quad (15, 2, -5)$$

y tantas otras resultan de éstas, si se cambian los signos de los términos extremos, por ejemplo $(-1, 8, 15)$, $(-2, 7, 15)$, etc., de tal suerte que todas son treinta y ocho. Pero rechazadas estas seis: $(\pm 13, 1, \mp 6)$, $(\pm 14, 3, \mp 5)$ y $(\pm 15, 2, \mp 5)$, las restantes treinta y dos comprenderán todas las reducidas.

Por el segundo método, tendremos las mismas formas en el orden siguiente*):

$$(\pm 7, 3, \mp 10), \quad (\pm 10, 3, \mp 7), \quad (\pm 7, 4, \mp 9), \quad (\pm 9, 4, \mp 7), \quad (\pm 6, 5, \mp 9),$$

*) Para $b = 1$, -78 no puede resolverse en dos factores que sin considerar el signo estén situados entre $\sqrt{79} + 1$ y $\sqrt{79} - 1$; por lo cual este valor es omitido, y, por la misma razón, los valores 2 y 6.

$$(\pm 9, 5, \mp 6), \quad (\pm 2, 7, \mp 15), \quad (\pm 3, 7, \mp 10), \quad (\pm 5, 7, \mp 6), \quad (\pm 6, 7, \mp 5),$$
$$(\pm 10, 7, \mp 3), \quad (\pm 15, 7, \mp 2), \quad (\pm 1, 8, \mp 15), \quad (\pm 3, 8, \mp 5),$$
$$(\pm 5, 8, \mp 3), \quad (\pm 15, 8, \mp 1)$$

186.

Sea F una forma reducida del determinante D y la forma F' contigua a ella misma por la parte última; entonces la reducida F'' será contigua a ésta por la parte última; la reducida F''' contigua a F'' por la parte última etc. Entonces, todas las formas F', F'', F''' etc. estarán completamente determinadas, y serán propiamente equivalentes tanto entre sí como a la forma F. Puesto que el número de todas las formas reducidas de determinante dado es finito, todas las formas en la progresión infinita F, F', F'' etc. no podrán ser diferentes. Supongamos que F^m y F^{m+n} son idénticas, entonces F^{m-1} y F^{m+n-1} serán reducidas, contiguas a la misma forma reducida por la parte primera, y por lo tanto idénticas. De la misma manera F^{m-2} y F^{m+n-2} serán idénticas, etc., y finalmente F y F^n. De este modo, en la progresión F, F', F'' etc., si se prosigue suficientemente, necesariamente vuelve a aparecer la primera forma F. Si suponemos que F^n es la primera idéntica a F, o sea todas F', F'', $\ldots F^{n-1}$ son diferentes de la forma F, se percibe que todas las formas F, F', F'', $\ldots F^{n-1}$ son diferentes. Llamaremos al conjunto de estas formas el *período de la forma* F. Por lo tanto, si la progresión se prolonga más allá de la última forma del período, del mismo modo tendremos de nuevo las formas F, F', F'' etc. y toda la progresión infinita F, F', F'' etc. estará constituida por este período de la forma F repetido infinitas veces.

La progresión F, F', F''etc. también puede prolongarse al revés, con anteponer a la forma F la reducida $'F$, la cual es contigua a F por la parte primera. Delante de ésta pondremos la reducida $''F$, la cual es contigua a ella por la primera parte etc. De esta manera se tiene una progresión de formas infinita *por ambos lados*:

$$\ldots {}''' F,\ {}'' F,\ {}' F,\ F,\ F',\ F'',\ F''' \ldots$$

Se ve que $'F$ será idéntica con F^{n-1}, $''F$ con F^{n-2} etc. y por lo tanto la progresión por el lado izquierdo también estará compuesta del período de la forma F repetida infinitas veces.

Si a las formas F, F', F'' etc. $'F$, $''F$, etc. se les atribuyen los índices 0, 1, 2, etc. -1, -2, etc. y en general a la forma F^m el índice m, a la forma ${}^m F$ el índice

$-m$, entonces *formas cualesquiera de la serie serán idénticas o diferentes, según los índices de ellas mismas sean congruentes o incongruentes según el módulo* n.

Ejemplo. Para la forma $(3, 8, -5)$, cuyo determinante es $= 79$, se encuentra este período: $(3, 8, -5)$, $(-5, 7, 6)$, $(6, 5, -9)$, $(-9, 4, 7)$, $(7, 3, -10)$, $(-10, 7, 3)$. Después de la última, de nuevo tenemos $(3, 8, -5)$. Así pues $n = 6$.

187.

Tenemos aquí algunas observaciones generales sobre estos períodos

1) Si las formas F, F', F'' etc.; $'F$, $''F$, $'''F$ etc. se presentan así:

$$(a, b, -a'),\ (-a', b', a''),\ (a'', b'', -a''') \text{ etc.}$$
$$(-'a,' b, a),\ (''a,'' b, -'a),\ (-'''a,''' b,'' a)$$

todos los a, a', a'', a''' etc. y $'a$, $''a$, $'''a$ etc. tendrán *el mismo signo* (artículo 184, proposición 1), y todos los b, b', b'' etc. $'b$, $''b$ etc. serán positivos.

2) De esto es evidente que el número n (el número de formas de las cuales está compuesto el período de la forma F) siempre es *par*. Pues el primer término de la forma F^m de este período tendrá el mismo signo que el primer término a de la forma F si m es par; el signo opuesto si m es impar. Puesto que F^n y F son idénticas, n será necesariamente par.

3) El algoritmo mediante el cual se encuentran los números b', b'', b''' etc., a'', a''' etc., por la proposición 6 del artículo 184, es éste:

$$b' \equiv -b \pmod{a'} \quad \text{entre los límites } \sqrt{D} \text{ y } \sqrt{D} \mp a'; \qquad a'' = \frac{D - b'^2}{a'}$$
$$b'' \equiv -b' \pmod{a''} \quad \ldots\ldots\ldots\ldots \sqrt{D} \mp a''; \qquad a''' = \frac{D - b''^2}{a''}$$
$$b''' \equiv -b'' \pmod{a'''} \ldots\ldots\ldots\ldots \sqrt{D} \mp a'''; \quad a'''' = \frac{D - b'''^2}{a'''}$$
$$\text{etc.}$$

donde en la segunda columna, el signo superior o el inferior debe tomarse, según a, a', a'' etc. sean positivos o negativos. En lugar de las fórmulas en la tercera columna,

pueden darse las siguientes, las cuales llegan a ser más cómodas, cuando D es un número grande:

$$a'' = \frac{b+b'}{a'}(b-b') + a$$
$$a''' = \frac{b'+b''}{a''}(b'-b'') + a'$$
$$a'''' = \frac{b''+b'''}{a'''}(b''-b''') + a''$$
etc.

4) Una forma cualquiera F^m, contenida en el período de la forma F, tiene el mismo período que F. A saber, este período será F^m, F^{m+1}, $\ldots F^{n-1}$, F, F', $\ldots F^{m-1}$, en el cual aparecen las mismas formas y en el mismo orden que en el período de la forma F. Este discrepa de aquél únicamente respecto del inicio y del fin.

5) Es claro que todas las formas reducidas de un mismo determinante D pueden *distribuirse* en períodos. Tómese libremente alguna de estas formas F y búsquese su período F, F', F'', $\ldots F^{n-1}$, el cual denotaremos por P. Si no se comprenden todas las formas reducidas del determinante D, sea G alguna no contenida en él, y sea Q el período de ella. Entonces, es claro que P y Q no podrán tener ninguna forma común; de otra manera G tendría que estar contenida también en P y los períodos coincidirán totalmente. Si P y Q aún no agotan todas las formas reducidas, alguna de las faltantes, H, suministrará un tercer período, R, el cual no tendrá una forma en común con P y tampoco con Q. Podemos continuar en esta manera hasta agotar todas las formas reducidas. Por ejemplo, todas las formas reducidas del determinante 79 se distribuyen en seis períodos:

I. $(1,8,-15)$, $(-15,7,2)$, $(2,7,-15)$, $(-15,8,1)$.
II. $(-1,8,15)$, $(15,7,-2)$, $(-2,7,15)$, $(15,8,-1)$.
III. $(3,8,-5)$, $(-5,7,6)$, $(6,5,-9)$, $(-9,4,7)$, $(7,3,-10)$, $(-10,7,3)$.
IV. $(-3,8,5)$, $(5,7,-6)$, $(-6,5,9)$, $(9,4,-7)$, $(-7,3,10)$, $(10,7,-3)$.
V. $(5,8,-3)$, $(-3,7,10)$, $(10,3,-7)$, $(-7,4,9)$, $(9,5,-6)$, $(-6,7,5)$.
VI. $(-5,8,3)$, $(3,7,-10)$, $(-10,3,7)$, $(7,4,-9)$, $(-9,5,6)$, $(6,7,-5)$.

6) Llamaremos *formas asociadas* a las que constan de los mismos términos, pero puestos en orden inverso, como $(a,b,-a')$, $(-a',b,a)$. Entonces, se percibe de la proposición 7 del artículo 184 que si el período de la forma reducida F es F, F',

F'', $\ldots F^{n-1}$, y si la forma f es asociada a F y las formas f', f'', $\ldots f^{n-2}$, f^{n-1} son asociadas a las formas F^{n-1}, F^{n-2}, $\ldots F''$, F', respectivamente, entonces el período de la forma f será f, f', f'', $\ldots f^{n-2}$, f^{n-1}, y por lo tanto constará de tantas formas como el período de la forma F. Llamaremos *períodos asociados* a aquéllos de las formas asociadas. Así, en nuestro ejemplo, son asociados los períodos III y VI, IV y V.

7) Pero puede ser que la forma f aparezca en el período de su asociado F, como en nuestro ejemplo de los períodos I y II y, por tanto, el período de la forma F concuerde con el período de la forma f, o sea que *el período de la forma F sea asociado a sí mismo.* Cada vez que esto suceda se encontrarán dos formas ambiguas en este período. Supongamos que el período de la forma F consta de $2n$ formas, o sea F y F^{2n} son idénticas, y sea $2m+1$ el índice de la forma f en el período de la forma F *), o sea F^{2m+1} y F son asociadas. Entonces es claro que también F' y F^{2m} serán asociadas, además de F'' y F^{2m-1} etc., y por tanto F^m y F^{m+1}. Sea $F^m = (a^m, b^m, -a^{m+1})$, $F^{m+1} = (-a^{m+1}, b^{m+1}, a^{m+2})$. Entonces tendremos $b^m + b^{m+1} \equiv 0 \pmod{a^{m+1}}$; de la definición de las formas asociadas será $b^m = b^{m+1}$ y de esto $2b^{m+1} \equiv 0 \pmod{a^{m+1}}$, o sea la forma F^{m+1} es ambigua. Del mismo modo F^{2m+1} y F^{2n} serán asociadas; de esto F^{2m+2} y F^{2n-1}; F^{2m+3} y F^{2n-2} etc., finalmente F^{m+n} y F^{m+n+1}, de las cuales la segunda será ambigua, como se prueba con facilidad por razonamiento semejante. Dado que $m+1$ y $m+n+1$ son incongruentes según el módulo $2n$, las formas F^{m+1} y F^{m+n+1} no serán idénticas (artículo 186, donde n denota lo mismo que $2n$ aquí). Así en I, las formas ambiguas son $(1, 8, -15)$, $(2, 7, -15)$, en II son $(-1, 8, 15)$, $(-2, 7, 15)$.

8) Viceversa, *cada período, en el cual aparece una forma ambigua, es asociado a sí mismo.* En efecto, se ve que, si F^m es una forma reducida ambigua, a la vez la forma será contigua a su asociada (que también es reducida) por la parte primera, i.e., F^{m-1} y F^m son asociadas. Entonces todo el período será asociado a sí mismo. Es claro que *no puede ser que sólo una forma ambigua esté contenida en algún período.*

9) Tampoco puede haber *más de dos en un mismo período.* Supongamos que en el período de la forma F, compuesta de $2n$ formas, se presentan tres formas ambiguas F^λ, F^μ y F^ν, pertenecientes a los índices λ, μ y ν, respectivamente de tal manera que λ, μ y ν sean números diferentes situados entre los límites 0 y $2n-1$

*) Aquí el índice necesariamente será impar; puesto que los primeros términos de las formas F y f tienen signos opuestos (véase la observación 2 arriba).

(inclusive). Entonces las formas $F^{\lambda-1}$ y F^{λ} serán asociadas; y al mismo tiempo $F^{\lambda-2}$ y $F^{\lambda+1}$ etc., y finalmente F y $F^{2\lambda-1}$. Por el mismo razonamiento, F y $F^{2\mu-1}$ serán asociadas, además de F y $F^{2\nu-1}$; por lo cual $F^{2\lambda-1}$, $F^{2\mu-1}$ y $F^{2\nu-1}$ serán idénticas, y los índices $2\lambda-1$, $2\mu-1$, $2\nu-1$ serán congruentes, según el módulo $2n$, y por eso también $\lambda \equiv \mu \equiv \nu \pmod{n}$, *Q. E. A.* , puesto que claramente no pueden caer entre los límites 0 y $2n-1$ tres números diferentes congruentes, según el módulo n.

188.

Puesto que todas las formas del mismo período son propiamente equivalentes, la pregunta que surge es cuáles formas de diferentes períodos pueden ser también equivalentes. Pero antes de mostrar que *esto es imposible,* debemos decir algo acerca de la transformación de las formas reducidas.

Puesto que la transformación de formas frecuentemente será tratada abajo, evitaremos la prolijidad tanto como sea posible y usaremos el siguiente método más corto de escribir. Si la forma $LX^2+2MXY+NY^2$ es transformada en la forma $lx^2+2mxy+ny^2$ por la sustitución $X=\alpha x+\beta y$, $Y=\gamma x+\delta y$, diremos simplemente que (L,M,N) es transformada en (l,m,n) por la sustitución α, β, γ, δ. De esta manera no será necesario denotar por caracteres propios las incógnitas de cada una de las formas que están siendo tratadas. Es obvio que la *primera* incógnita deberá distinguirse bien de la *segunda* en cualquier forma.

Sea $(a,b,-a')\ldots f$ una forma reducida dada con determinante D. Como en el artículo 186, formamos una serie de formas reducidas infinita en ambas direcciones $\ldots {}''f, {}'f, f, f', f'', \ldots$ y sea

$$\begin{aligned} f' &= (-a', b', a''), \quad f'' = (a'', b'', -a''') \quad \text{etc.} \\ {}'f &= (-'a,' b, a), \quad {}''f = ({}''a,'' b, -'a) \quad \text{etc.} \end{aligned}$$

Póngase

$$\begin{aligned} \tfrac{b+b'}{-a'} &= h', \quad \tfrac{b'+b''}{a''} = h'', \quad \tfrac{b''+b'''}{-a'''} = h''' \quad \text{etc.} \\ \tfrac{'b+b}{a} &= h, \quad \tfrac{''b+'b}{-'a} =' h, \quad \tfrac{'''b+''b}{''a} ='' h \quad \text{etc.} \end{aligned}$$

Entonces es claro que si (como en artículo 177) los números α', α'', α''', etc., β', β'',

β''', etc., etc., son formados según el siguiente algoritmo

$$\begin{array}{llll}
\alpha' = 0 & \beta' = -1 & \gamma' = 1 & \delta' = h' \\
\alpha'' = \beta' & \beta'' = h''\beta' & \gamma'' = \delta' & \delta'' = h''\delta' - 1 \\
\alpha''' = \beta'' & \beta''' = h'''\beta'' - \beta' & \gamma''' = \delta'' & \delta''' = h'''\delta'' - \delta' \\
\alpha'''' = \beta''' & \beta'''' = h''''\beta''' - \beta'' & \gamma'''' = \delta''' & \delta'''' = h''''\delta''' - \delta''
\end{array}$$

etc.

f será transformada

$$\begin{array}{lll}
\text{en } f' & \text{por la sustitución} & \alpha',\ \beta',\ \gamma',\ \delta' \\
\text{en } f'' & \ldots\ldots\ldots & \alpha'',\ \beta'',\ \gamma'',\ \delta'' \\
\text{en } f''' & \ldots\ldots\ldots & \alpha''',\ \beta''',\ \gamma''',\ \delta'''
\end{array}$$

etc.

y todas estas transformaciones serán propias.

Puesto que $'f$ se transforma en f por la sustitución propia $0,\ -1,\ 1,\ h$ (art. 158), f será transformada en $'f$ por la sustitución propia $h,\ 1,\ -1,\ 0$. Por razonamiento similar, $'f$ será transformada en $''f$ por la sustitución propia $'h,\ 1,\ -1,\ 0$; $''f$ en $'''f$ por la sustitución propia $''h,\ 1,\ -1,\ 0$ etc. De esto, por el artículo 159, concluimos, de la misma forma como en el artículo 177, que si los números $'\alpha$, $''\alpha$, $'''\alpha$, etc., $'\beta$, $''\beta$, $'''\beta$, etc., etc., son formados según el siguiente algoritmo

$$\begin{array}{llll}
'\alpha = h & '\beta = 1 & '\gamma = -1 & '\delta = 0 \\
''\alpha = 'h'\alpha - 1 & ''\beta = '\alpha & ''\gamma = 'h'\gamma & ''\delta = '\gamma \\
'''\alpha = ''h''\alpha - '\alpha & '''\beta = ''\alpha & '''\gamma = ''h''\gamma - '\gamma & '''\delta = ''\gamma \\
''''\alpha = '''h'''\alpha - ''\alpha & ''''\beta = '''\alpha & ''''\gamma = '''h'''\gamma - ''\gamma & ''''\delta = '''\gamma
\end{array}$$

etc.

entonces f será transformada

$$\begin{array}{lll}
\text{en } 'f & \text{por la sustitución} & '\alpha,\ '\beta,\ '\gamma,\ '\delta \\
\text{en } ''f & \ldots\ldots\ldots & ''\alpha,\ ''\beta,\ ''\gamma,\ ''\delta \\
\text{en } '''f & \ldots\ldots\ldots & '''\alpha,\ '''\beta,\ '''\gamma,\ '''\delta
\end{array}$$

etc.

y todas estas transformaciones serán propias.

Si se pone $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\delta = 1$, estos números tendrán la misma relación con la forma f que α', β', γ', δ' tienen con f'; α'', β'', γ'', δ'' tiene con f'' etc.; $'\alpha$, $'\beta$, $'\gamma$, $'\delta$ con $'f$ etc. Es decir, por la sustitución α, β, γ, δ la forma f será transformada en f. Entonces las series infinitas α', α'', α''', etc., $'\alpha$, $''\alpha$, $'''\alpha$ etc. serán claramente puestas juntas por la inserción del término α de modo que puedan ser concebidas como una serie infinita continua en ambas direcciones de acuerdo a la ley de progresión $\ldots, '''\alpha, ''\alpha, '\alpha, \alpha, \alpha', \alpha'', \alpha''', \ldots$. La ley de progresión es la siguiente

$$'''\alpha + '\alpha = ''h''\alpha,\ ''\alpha + \alpha = 'h'\alpha,\ '\alpha + \alpha' = h\alpha,\ \alpha + \alpha'' = h'\alpha',\ \alpha' + \alpha''' = h''\alpha'' \text{ etc.}$$

o en general (si suponemos que un índice negativo indica la misma cosa escrito a la derecha que un índice positivo escrito en la izquierda)

$$\alpha^{m-1} + \alpha^{m+1} = h^m \alpha^m$$

De una manera similar la serie $\ldots, ''\beta, 'beta, \beta, \beta', \beta'', \ldots$ será continua, y su ley es

$$\beta^{m-1} + \beta^{m+1} = h^{m+1}\beta^m$$

Esta serie es idéntica a la precedente si cada término es movido hacia arriba un lugar $''\beta = '\alpha$, $'\beta = \alpha$, $\beta = \alpha'$, etc. La ley para la serie continua $\ldots, ''\gamma, 'gamma, \gamma, \gamma', \gamma'', \ldots$ será

$$\gamma^{m-1} + \gamma^{m+1} = h^m \gamma^m$$

y la ley para $\ldots, ''\delta, 'delta, \delta, \delta', \delta'', \ldots$ será

$$\delta^{m-1} + \delta^{m+1} = h^{m+1}\delta^m$$

y generalmente $\delta^m = \gamma^{m+1}$.

Ejemplo. Sea f la forma $(3, 8, -5)$ la cual se transformará

en la forma $''''''f$	$(-10, 7, 3)$	por la sustitución	$-805, -152, +143, +27$
$''''''f$	$(3, 8, -5)$		$-152, +45, +27, -8$
$''''f$	$(-5, 7, 6)$		$+45, +17, -8, -3$
$''''f$	$(6, 5, -9)$		$+17, -11, -3, +2$
$'''f$	$(-9, 4, 7)$		$-11, -6, +2, +1$
$''f$	$(7, 3, -10)$		$-6, +5, +1, -1$
$'f$	$(-10, 7, 3)$		$+5, +1, -1, 0$
f	$(3, 8, -5)$		$+1, 0, 0, +1$
f'	$(-5, 7, 6)$		$0, -1, +1, -3$
f''	$(6, 5, -9)$		$-1, -2, -3, -7$
f'''	$(-9, 4, 7)$		$-2, +3, -7, +10$
f''''	$(7, 3, -10)$		$+3, +5, +10, +17$
f'''''	$(-10, 7, 3)$		$+5, -8, +17, -27$
f''''''	$(3, 8, -5)$		$-8, -45, -27, -152$
f'''''''	$(-5, 7, 6)$		$-45, +143, -152, +483$

etc.

189.

Lo siguiente debe ser notado con relación a este algoritmo.

1) Todos los números a, a', a'', etc., $'a$, $''a$, etc., tendrán el mismo signo; todos los números b, b', b'', etc., $'b$, $''b$, etc. serán positivos; en la serie $\ldots ''h, 'h, h, h', h'', \ldots$ alternarán los signos, esto es, si todos los a, a', etc., son positivos, h^m o ${}^m h$ será positivo cuando m sea par, negativo cuando m sea impar; pero si a, a', etc., son negativos h^m o ${}^m h$ será negativo para m par, positivo para m impar.

2) Si a es positivo y entonces h' es negativo, h'' es positivo etc., vamos a tener $\alpha'' = -1$ negativo, $\alpha''' = h''\alpha''$ negativo y $> \alpha''$ (o $= \alpha''$ si $h'' = 1$); $\alpha'''' = h'''\alpha''' - \alpha''$ es positivo y $> \alpha'''$ (porque $h'''\alpha'''$ positivo, α'' negativo); $\alpha''''' = h''''\alpha'''' - \alpha'''$ positivo y $> \alpha''''$ (porque $h''''\alpha''''$ es positivo) etc. Es entonces fácil de concluir que la serie α', α'', α''', etc., crecerá sin cota y que siempre habrá dos signos positivos y dos negativos tal que α^m tiene el signo $+, +, -, -$ según sea $m \equiv 0, 1, 2, 3 \pmod 4$. Si a es

negativo, por un razonamiento parecido encontramos α'' negativo, α''' positivo y $>$ ó $= \alpha''$; α'''' positivo $> \alpha'''$; α''''' negativo $> \alpha''''$; etc., de modo que la serie α', α'', α''', etc., crezca contínuamente, y el signo del término α^m será $+,\ -,\ -,\ +$, según sea $m \equiv 0,\ 1,\ 2,\ 3 \pmod 4$

3) De esta forma encontramos que las cuatro progresiones α', α'', α''', etc., γ, γ', γ'', etc., α', α, $'\alpha$, $''\alpha$, etc., γ, $'\gamma$, $''\gamma$, etc., crecen contínuamente y entonces todas las siguientes, que son idénticas a ellas: β, β', β'', etc., $'\delta$, δ, δ', δ'', etc., β, $'\beta$, $''\beta$, etc., $'\delta$, $''\delta$, etc., y según sea $m \equiv 0,\ 1,\ 2,\ 3 \pmod 4$, el signo

$$\begin{array}{ll} \text{de } \alpha^m, + \pm - \mp; & \text{de } \beta^m, \pm - \mp + \\ \text{de } \gamma^m, \pm + \mp -; & \text{de } \delta^m, + \mp - \pm \\ \text{de } {}^m\alpha, + \pm - \mp; & \text{de } {}^m\beta, \mp + \pm - \\ \text{de } {}^m\gamma, \mp - \pm +; & \text{de } {}^m\delta, + \mp - \pm \end{array}$$

con el signo superior usado cuando a es positivo, el inferior cuando a es negativo. Téngase en cuenta esta propiedad: si designamos cualquier índice positivo por m, α^m y γ^m tendrán el mismo signo cuando a es positivo, signos opuestos cuando a es negativo, y similarmente para β^m y δ^m; por el otro lado ${}^m\alpha$ y ${}^m\gamma$ o ${}^m\beta$ y ${}^m\delta$ tendrán el mismo signo cuando a es negativo, opuesto cuando a es positivo.

4) Usando la notación del artículo 27 podemos mostrar el tamaño de los números α^m etc., poniendo

$$\mp h' = k', \quad \pm h'' = k'', \quad \mp h''' = k''' \text{ etc.} \quad \pm h = k, \quad \mp' h = {}'k, \quad \pm'' h = {}''k \quad \text{etc.}$$

tal que todos los números k', k'', etc.; k, $'k$, etc., sean positivos:

$$\begin{array}{ll} \alpha^m = \pm[k'', k''', k'''', \ldots k^{m-1}]; & \beta^m = \pm[k'', k''', k'''', \ldots k^m] \\ \gamma^m = \pm[k', k'', k''', \ldots. k^{m-1}]; & \delta^m = \pm[k', k'', k''', \ldots. k^m] \\ {}^m\alpha = \pm[k, {}'k, {}''k, \ldots. {}^{m-1}k]; & {}^m\beta = \pm[k, {}'k, {}''k, \ldots {}^{m-2}k] \\ {}^m\gamma = \pm[{}'k, {}''k, \ldots\ldots {}^{m-1}k]; & {}^m\delta = \pm[{}'k, {}''k, \ldots. {}^{m-2}k] \end{array}$$

Los *signos* deberán ser determinados por lo que acabamos de decir arriba. A través de estas fórmulas, cuya demostración omitiremos por ser muy fácil, el cómputo involucrado puede hacerse muy rápidamente.

190.

LEMA: *Designemos enteros cualesquiera por las letras* m, μ, m', n, ν, n' *de tal forma que ninguno de los últimos tres sea* $= 0$. *Afirmo que si* $\frac{\mu}{\nu}$ *está estrictamente entre los límites* $\frac{m}{n}$ *y* $\frac{m'}{n'}$ *y si* $mn' - nm' = \mp 1$, *entonces el denominador* ν *será mayor que* n *y* n'.

Demostración. Manifiestamente $\mu nn'$ estará entre $\nu mn'$ y $\nu nm'$, y entonces la diferencia entre este número y cada límite será menor que la diferencia entre un límite y el otro; i.e., tenemos $\nu mn' - \nu nm' > \mu nn' - \nu mn'$ y $> \mu nn' - \nu nm'$, o $\nu > n'(\mu n - \nu m)$ y $> n(\mu n' - \nu m')$. Entonces se sigue que, puesto que $\mu n - \nu m$ no es $= 0$ (puesto que de otra manera tendríamos $\frac{\mu}{\nu} = \frac{m}{n}$ contrariamente a la hipótesis) y tampoco $\mu n' - \nu m' = 0$ (por una razón similar), pero cada uno será al menos $= 1$, por lo tanto $\nu > n'$ y $> n$. *Q. E. D.*

Es por lo tanto claro que ν no puede ser $= 1$; i.e., si $mn' - nm' = \pm 1$ ningún entero puede estar entre las fracciones $\frac{m}{n}$ y $\frac{m'}{n'}$. Tampoco cero puede estar entre ellas, i.e., las fracciones no pueden tener signos contrarios.

191.

TEOREMA. *Si la forma reducida* $(a, b, -a')$ *con determinante* D *es transformada por la sustitución* α, β, γ, δ *en la forma reducida* $(A, B, -A')$ *con el mismo determinante:* Primero, $\frac{\pm\sqrt{D}-b}{a}$ *estará entre* $\frac{\alpha}{\gamma}$ *y* $\frac{\beta}{\delta}$ *(siempre y cuando ni* γ *ni* $\delta = 0$, *i.e., si cada límite es finito). El signo superior debe ser usado cuando ninguno de estos límites tiene un signo contrario al de* a *(o más claro, cuando ambos tienen el mismo signo o uno tiene el mismo signo, el otro* $= 0$*). El signo inferior debe ser usado cuando ninguno tiene el mismo signo de* a. Segundo, $\frac{\pm\sqrt{D}+b}{a'}$ *estará entre* $\frac{\gamma}{\alpha}$ *y* $\frac{\delta}{\beta}$ *(siempre y cuando ni* α *ni* $\beta = 0$*). El signo superior debe ser usado cuando ningún límite tiene un signo contrario al signo de* a' *(o* a*), el signo inferior cuando ninguno tiene el mismo signo de* a' **).*

Demostración. Tenemos las ecuaciones

$$a\alpha^2 + 2b\alpha\gamma - a'\gamma^2 = A \qquad [1]$$

$$a\beta^2 + 2b\beta\delta - a'\delta^2 = -A' \qquad [2]$$

---

*) No puede haber otros casos ya que, según el artículo anterior, $\alpha\delta - \beta\gamma = \pm 1$, y entonces los dos límites no pueden tener signos opuestos ni ser simultáneamente cero.

De esto deducimos

$$\frac{\alpha}{\gamma} = \frac{\pm\sqrt{D + \frac{aA}{\gamma^2}} - b}{a} \quad [3]$$

$$\frac{\beta}{\delta} = \frac{\pm\sqrt{D - \frac{aA'}{\delta^2}} - b}{a} \quad [4]$$

$$\frac{\gamma}{\alpha} = \frac{\pm\sqrt{D - \frac{a'A}{\alpha^2}} + b}{a'} \quad [5]$$

$$\frac{\delta}{\beta} = \frac{\pm\sqrt{D + \frac{a'A'}{\beta^2}} + b}{a'} \quad [6]$$

Las ecuaciones [3], [4], [5], [6] deben descartarse si γ, δ, α, β son respectivamente $= 0$. Pero todavía queda la duda acerca de cuáles *signos* deben darse a las cantidades en radicales. Vamos a decidir esto de la siguiente manera.

Es claro inmediatamente que con [3] y [4] el signo de arriba debe ser usado cuando ni $\frac{\alpha}{\gamma}$ ni $\frac{\beta}{\delta}$ tengan un signo contrario al de a, porque si el signo inferior fuera usado, $\frac{a\alpha}{\gamma}$ y $\frac{a\beta}{\delta}$ serían cantidades negativas. Ahora, puesto que A y A' tienen el mismo signo, $\sqrt{D}$ cae entre $\sqrt{D + \frac{aA}{\gamma^2}}$ y $\sqrt{D - \frac{aA'}{\delta^2}}$ y así en este caso $\frac{\sqrt{D}-b}{a}$ caerá entre $\frac{\alpha}{\gamma}$ y $\frac{\beta}{\delta}$. Entonces la primera parte del teorema ha sido demostrada para el caso anterior.

De la misma manera vemos que en [5] y [6] los signos inferiores deben tomarse cuando ni $\frac{\gamma}{\alpha}$ ni $\frac{\delta}{\beta}$ tenga el mismo signo de a' o a, porque si tomamos el signo superior, $\frac{a'\gamma}{\alpha}$ y $\frac{a'\delta}{\beta}$ serían necesariamente cantidades positivas. Entonces sucedería en este caso que $\frac{-\sqrt{D}+b}{a'}$ estaría entre $\frac{\gamma}{\alpha}$ y $\frac{\delta}{\beta}$. Por lo tanto la segunda parte del teorema queda mostrada para el último caso. Ahora, si hubiera sido igualmente fácil mostrar que en [3] y [4] los signos inferiores deberían ser tomados cuando ninguna de las cantidades $\frac{\alpha}{\gamma}$ y $\frac{\beta}{\delta}$ tiene el mismo signo de a, y los signos superiores en [5] y [6] cuando ni $\frac{\gamma}{\alpha}$ ni $\frac{\delta}{\beta}$ tienen signo opuesto, entonces se seguiría para el primer caso que $\frac{-\sqrt{D}-b}{a}$ está entre $\frac{\alpha}{\gamma}$ y $\frac{\beta}{\delta}$ y para el último caso que $\frac{\sqrt{D}+b}{a'}$ está entre $\frac{\gamma}{\alpha}$ y $\frac{\delta}{\beta}$; es decir, la primera parte del teorema quedaría demostrada para el último caso y la segunda parte para el primer caso. Pero aunque esto no es difícil, no se puede hacer sin algunas ambigüedades y preferimos entonces el siguiente método.

Cuando ninguno de los números α, β, γ, $\delta = 0$, entonces $\frac{\alpha}{\gamma}$ y $\frac{\beta}{\delta}$ tendrán los mismos signos que $\frac{\gamma}{\alpha}$ y $\frac{\delta}{\beta}$. Cuando, por lo tanto, ninguna de estas cantidades tiene el

mismo signo que a' o a, y entonces $\frac{-\sqrt{D}+b}{a'}$ está entre $\frac{\gamma}{\alpha}$ y $\frac{\delta}{\beta}$, ninguna de las cantidades $\frac{\alpha}{\gamma}$ y $\frac{\beta}{\delta}$ tendrá el mismo signo de a y $\frac{a'}{-\sqrt{D}+b} = \frac{-\sqrt{D}-b}{a}$ (puesto que $aa' = D - b^2$) estarán entre $\frac{\alpha}{\gamma}$ y $\frac{\beta}{\delta}$. Por lo tanto para el caso en que ni α ni $\beta = 0$, la primera parte del teorema cubre el segundo caso (pues la condición que ni γ ni $\delta = 0$ ha sido considerada en el mismo teorema). De una forma similar cuando ninguno de los números α, β, γ, $\delta = 0$ y ni $\frac{\alpha}{\gamma}$ ni $\frac{\beta}{\delta}$ tiene el signo opuesto a a o a', y por eso $\frac{\sqrt{D}-b}{a'}$ está entre $\frac{\alpha}{\gamma}$ y $\frac{\beta}{\delta}$, entonces ni $\frac{\gamma}{\alpha}$ ni $\frac{\delta}{\beta}$ tendrán un signo opuesto al de a', y $\frac{a}{\sqrt{D}-b} = \frac{\sqrt{D}+b}{a'}$ estará entre $\frac{\gamma}{\alpha}$ y $\frac{\delta}{\beta}$. Por lo tanto, donde ni γ ni $\delta = 0$ la segunda parte del teorema demuestra el segundo caso.

Queda entonces por mostrar que la primera parte del teorema también se aplica al segundo caso si ninguno de los números α y $\beta = 0$, y que la segunda parte se aplica al primer caso si γ o $\delta = 0$. Pero *todos estos casos son imposibles.* Supóngase, pues, para la *primera* parte del teorema que ni γ ni $\delta = 0$; que $\frac{\alpha}{\gamma}$ y $\frac{\beta}{\delta}$ no tienen el mismo signo que a y que (1) $\alpha = 0$. Entonces, de la ecuación $\alpha\delta - \beta\gamma = \pm 1$ tenemos $\beta = \pm 1$, $\gamma = \pm 1$. Y de [1] $A = -a'$, por lo tanto A y a' y entonces también a y A' tendrán signos opuestos y $\sqrt{D - \frac{aA'}{\delta^2}} > \sqrt{D} > b$. De esto es claro que en [4] se toma necesariamente el signo inferior porque, si tomamos el signo superior, $\frac{\beta}{\delta}$ tendría el mismo signo que a. Tenemos entonces $\frac{\beta}{\delta} > \frac{-\sqrt{D}-b}{a} > 1$ (puesto que $a < \sqrt{D} + b$ por la definición de una forma reducida), *Q. E. A.* , pues $\beta = \pm 1$, y δ no es $= 0$. (2) Sea $\beta = 0$, entonces, por la ecuación $\alpha\delta - \beta\gamma = \pm 1$ tenemos $\alpha = \pm 1$, $\delta = \pm 1$. De [2] $-A' = -a'$, así a', a y A tendrán el mismo signo y $\sqrt{D + \frac{aA}{\alpha^2}} > \sqrt{D} > b$. Por lo tanto claramente en [3] tenemos que tomar el signo inferior porque si tomamos el signo superior, $\frac{\alpha}{\gamma}$ tendría el mismo signo de a. Obtenemos entonces $\frac{\alpha}{\gamma} > \frac{-\sqrt{D}-b}{a} > 1$, *Q. E. A.* , por la misma razón de antes. Para la *segunda* parte, si suponemos que ni α ni $\beta = 0$; que $\frac{\gamma}{\alpha}$ y $\frac{\delta}{\beta}$ no tienen signos opuestos al de a' y que (1) $\gamma = 0$: de la ecuación $\alpha\delta - \beta\gamma = \pm 1$ obtenemos $\alpha = \pm 1$, $\delta = \pm 1$. Entonces por [1] $A = a$ y a' y A' tendrán el mismo signo y entonces $\sqrt{D + \frac{a'A'}{\beta^2}} > \sqrt{D} > b$. Por lo tanto en [6] se tiene que tomar el signo superior porque si tomamos el signo de abajo, $\frac{\delta}{\beta}$ tendría un signo opuesto al de a'. Obtenemos entonces $\frac{\delta}{\beta} > \frac{\sqrt{D}+b}{a'} > 1$, *Q. E. A.* , porque $\delta = \pm 1$ y β no es $= 0$. Finalmente (2), si fuera $\delta = 0$, de $\alpha\delta - \beta\gamma = \pm 1$ tendríamos $\beta = \pm 1$, $\gamma = \pm 1$ y así de [2] $-A' = a$. Por lo tanto $\sqrt{D - \frac{a'A}{\alpha^2}} > \sqrt{D} > b$, y se debe tomar el signo superior en [5]; $\frac{\gamma}{\alpha} > \frac{\sqrt{D}+b}{a'} > 1$, *Q. E. A.* Y el teorema está demostrado en toda su generalidad.

Puesto que la diferencia entre $\frac{\alpha}{\gamma}$ y $\frac{\beta}{\delta}$ es $= \frac{1}{\gamma\delta}$, la diferencia entre $\frac{\pm\sqrt{D}-b}{a}$ y $\frac{\alpha}{\gamma}$ o $\frac{\beta}{\delta}$ será $< \frac{1}{\gamma\delta}$; entonces, entre $\frac{\pm\sqrt{D}-b}{a}$ y $\frac{\alpha}{\gamma}$ o entre esa cantidad y $\frac{\beta}{\delta}$ no puede haber fracciones cuyo denominador no sea mayor que γ o δ (*lema precedente*). De la misma manera, la diferencia entre la cantidad $\frac{\pm\sqrt{D}+b}{a}$ y la fracción $\frac{\gamma}{\alpha}$ o $\frac{\delta}{\beta}$ será menor que $\frac{1}{\alpha\beta}$, y ninguna fracción puede estar entre esa cantidad y alguna de estas fracciones a no ser que el denominador sea mayor que α y β.

192.

Con la aplicación del teorema precedente al algoritmo del artículo 188 se sigue que la cantidad $\frac{\sqrt{D}-b}{a}$, la cual designaremos con L, estará entre $\frac{\alpha'}{\gamma'}$ y $\frac{\beta'}{\delta'}$; entre $\frac{\alpha''}{\gamma''}$ y $\frac{\beta''}{\delta''}$; entre $\frac{\alpha'''}{\gamma'''}$ y $\frac{\beta'''}{\delta'''}$, etc. (puesto que es fácil de ver por el artículo 189.3, hacia el final, que ninguno de estos límites tiene un signo opuesto al de a, así, se debe dar un signo positivo a la cantidad radical $\sqrt{D}$); o entre $\frac{\alpha'}{\gamma'}$ y $\frac{\alpha''}{\gamma''}$; entre $\frac{\alpha''}{\gamma''}$ y $\frac{\alpha'''}{\gamma'''}$, etc. Por lo tanto todas las fracciones $\frac{\alpha'}{\gamma'}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha'''''}{\gamma'''''}$, etc. estarán en un lado de L, y todas las fracciones $\frac{\alpha''}{\gamma''}$, $\frac{\alpha''''}{\gamma''''}$, $\frac{\alpha''''''}{\gamma''''''}$, etc. en el otro lado. Pero, puesto que $\gamma' < \gamma'''$, $\frac{\alpha'}{\gamma'}$ estará *fuera* de $\frac{\alpha'''}{\gamma'''}$ y L, y por una razón análoga $\frac{\alpha''}{\gamma''}$ estará fuera de L y $\frac{\alpha''''}{\gamma''''}$; $\frac{\alpha'''}{\gamma'''}$ fuera de L y $\frac{\alpha'''''}{\gamma'''''}$; etc. Entonces estas cantidades están en el siguiente orden:

$$\frac{\alpha'}{\gamma'},\quad \frac{\alpha'''}{\gamma'''},\quad \frac{\alpha'''''}{\gamma'''''},\quad \ldots L,\quad \ldots\frac{\alpha''''''}{\gamma''''''},\quad \frac{\alpha''''}{\gamma''''},\quad \frac{\alpha''}{\gamma''}$$

La diferencia entre $\frac{\alpha'}{\gamma'}$ y L será menor que la diferencia entre $\frac{\alpha'}{\gamma'}$ y $\frac{\alpha''}{\gamma''}$; i.e. $< \frac{1}{\gamma'\gamma''}$, y por una razón análoga la diferencia entre $\frac{\alpha''}{\gamma''}$ y L será $< \frac{1}{\gamma''\gamma'''}$ etc. Por lo tanto, las fracciones $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, etc. se aproximarán continuamente al límite L y, puesto que γ', γ'', γ''' crecen indefinidamente, la diferencia entre las fracciones y el límite puede hacerse menor que cualquier cantidad dada.

Por el artículo 189, ninguna de las cantidades $\frac{\gamma}{\alpha}$, $\frac{'\gamma}{'\alpha}$, $\frac{''\gamma}{''\alpha}$, etc. tendrá el mismo signo que a; entonces, por el razonamiento de arriba, estos números y la cantidad $\frac{-\sqrt{D}+b}{a'}$, que designaremos por L', estarán en el siguiente orden:

$$\frac{\gamma}{\alpha},\quad \frac{''\gamma}{''\alpha},\quad \frac{''''\gamma}{''''\alpha},\quad \ldots L',\quad \ldots\frac{''''''\gamma}{''''''\alpha},\quad \frac{'''\gamma}{'''\alpha},\quad \frac{'\gamma}{'\alpha}$$

La diferencia entre $\frac{\gamma}{\alpha}$ y L' será menor que $\frac{1}{{}'\alpha\alpha}$, la diferencia entre $\frac{{}'\gamma}{{}'\alpha}$ y L' menor que $\frac{1}{{}''\alpha'\alpha}$, etc. Por lo tanto, las fracciones $\frac{\gamma}{\alpha}$, $\frac{{}'\gamma}{{}'\alpha}$, etc. se aproximarán continuamente a L' y la diferencia puede hacerse menor que cualquier cantidad dada.

En el ejemplo del artículo 188 tenemos $L = \frac{\sqrt{79}-8}{3} = 0,2960648$, y las fracciones aproximantes son $\frac{0}{1}$, $\frac{1}{3}$, $\frac{2}{7}$, $\frac{3}{10}$, $\frac{5}{17}$, $\frac{8}{27}$, $\frac{45}{152}$, $\frac{143}{483}$, etc., y $\frac{143}{483} = 0,2960662$. En el mismo ejemplo $L' = \frac{-\sqrt{79}+8}{5} = -0,1776388$, y las fracciones aproximantes son $\frac{0}{1}$, $-\frac{1}{5}$, $-\frac{1}{6}$, $-\frac{2}{11}$, $-\frac{3}{17}$, $-\frac{8}{45}$, $-\frac{27}{152}$, $-\frac{143}{805}$, etc. De hecho $\frac{143}{805} = 0,1776397$.

193.

TEOREMA. *Si las formas reducidas f y F son propiamente equivalentes, cada una de ellas estará contenida en el período de la otra.*

Sea $f = (a, b, -a')$ y $F = (A, B, -A')$ y el determinante de estas formas D, y transfórmese la primera en la segunda por la sustitución propia $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$. Si se busca el período de la forma f y se calcula la serie infinita de dos sentidos de las formas reducidas y las transformaciones de la forma f en éstas, como hicimos en el artículo 188, entonces *o bien* $+\mathfrak{A}$ será igual a algún término de la serie $\ldots''\alpha, {}'\alpha, \alpha, \alpha', \alpha'', \ldots$ (y si lo ponemos $= \alpha^m$, $+\mathfrak{B}$ será $= \beta^m$, $+\mathfrak{C} = \gamma^m$, $+\mathfrak{D} = \delta^m$); *o bien* $-\mathfrak{A}$ será igual a algún término α^m y $-\mathfrak{B}$, $-\mathfrak{C}$, $-\mathfrak{D}$, respectivamente, serán $= \beta^m$, γ^m, δ^m (donde m puede designar también un índice negativo). En cualquier caso F será idéntico a f^m.

Demostración. I. Tenemos las cuatro ecuaciones

$$a\mathfrak{A}^2 + 2b\mathfrak{A}\,\mathfrak{C} - a'\mathfrak{C}^2 = A \qquad [1]$$

$$a\mathfrak{A}\,\mathfrak{B} + b(\mathfrak{A}\,\mathfrak{D} + \mathfrak{B}\,\mathfrak{C}) - a'\mathfrak{C}\,\mathfrak{D} = B \qquad [2]$$

$$a\mathfrak{B}^2 + 2b\mathfrak{B}\,\mathfrak{D} - a'\mathfrak{D}^2 = -A' \qquad [3]$$

$$\mathfrak{A}\,\mathfrak{D} - \mathfrak{B}\,\mathfrak{C} = 1 \qquad [4]$$

Consideremos *primero* el caso donde uno de los números $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D} = 0$.

1^o Si $\mathfrak{A} = 0$ resulta por [4] $\mathfrak{B}\,\mathfrak{C} = -1$, y así $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$. Entonces por [1], $-a' = A$; por [2], $-b \pm a'\mathfrak{D} = B$ o $B \equiv -b \pmod{a' \text{ o } A}$; por lo tanto, se deduce que la forma $(A, B, -A')$ es contigua por la parte última a la forma $(a, b, -a')$. Puesto que la primera de éstas es reducida, será necesariamente idéntica a f'. Por lo tanto $B = b'$, y entonces de [2] $b + b' = -a'\mathfrak{C}\,\mathfrak{D} = \pm a'\mathfrak{D}$; de esto, puesto que $\frac{b+b'}{-a'} = h'$,

tenemos que $\mathfrak{D} = \mp h'$. De esto se colige que $\mp\mathfrak{A}$, $\mp\mathfrak{B}$, $\mp\mathfrak{C}$, $\mp\mathfrak{D}$ son respectivamente $= 0, -1, +1, h'$, o $= \alpha', \beta', \gamma', \delta'$.

2^o Si $\mathfrak{B} = 0$ tenemos de [4] $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; de [3] $a' = A'$; de [2] $b \mp a'\mathfrak{C} = B$, o $b \equiv B \pmod{a'}$. Pero, como f y F son formas reducidas, ambas b y B estarán entre $\sqrt{D}$ y $\sqrt{D} \mp a'$ (según a' sea positivo o negativo, por el art. 184.5). Así, será necesariamente, $b = B$ y $\mathfrak{C} = 0$. Entonces las formas f y F son idénticas y $\pm\mathfrak{A}$, $\pm\mathfrak{B}$, $\pm\mathfrak{C}$, $\pm\mathfrak{D} = 1, 0, 0, 1 = \alpha, \beta, \gamma, \delta$ respectivamente.

3^o Si $\mathfrak{C} = 0$ tenemos de [4] $\mathfrak{A} = \pm 1$, $\mathfrak{D} = \pm 1$; de [1] $a = A$; de [2] $\pm a\mathfrak{B} + b = B$ o $b \equiv B \pmod{a}$. Dado que tanto b como B están entre $\sqrt{D}$ y $\sqrt{D} \mp a$, necesariamente se tendrá que $B = b$ y $\mathfrak{B} = 0$. Así, este caso no difiere del precedente.

4^o Si $\mathfrak{D} = 0$, tenemos de [4] $\mathfrak{B} = \pm 1$, $\mathfrak{C} = \mp 1$; de [3] $a = -A'$; de [2] $\pm a\mathfrak{A} - b = B$ o $B \equiv -b \pmod{a}$. Entonces la forma F será contigua por la primera parte a la forma f y así idéntica a la forma $'f$. Por lo tanto, puesto que $\frac{'b+b}{a} = h$ y $B = 'b$ tenemos $\pm\mathfrak{A} = h$. De aquí se colige $\pm\mathfrak{A}$, $\pm\mathfrak{B}$, $\pm\mathfrak{C}$, $\pm\mathfrak{D}$ respectivamente $= h, 1, -1, 0 = '\alpha, '\beta, '\gamma, '\delta$.

Sólo queda el caso donde ninguno de los números $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D} = 0$. Por el lema del artículo 190, las cantidades $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\frac{\mathfrak{B}}{\mathfrak{D}}$, $\frac{\mathfrak{C}}{\mathfrak{A}}$, $\frac{\mathfrak{D}}{\mathfrak{B}}$ tendrán el mismo signo y resultarán dos casos según este signo sea el mismo o el opuesto al signo de a y a'.

II. Si $\frac{\mathfrak{A}}{\mathfrak{C}}$ y $\frac{\mathfrak{B}}{\mathfrak{D}}$ tienen el mismo signo que a, la cantidad $\frac{\sqrt{D}-b}{a}$ (la cual designaremos por L) estará entre estas fracciones (art. 191). Ahora demostraremos que $\frac{\mathfrak{A}}{\mathfrak{C}}$ es igual a una de las fracciones $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, $\frac{\alpha''''}{\gamma''''}$, etc. y $\frac{\mathfrak{B}}{\mathfrak{D}}$ a la siguiente; esto es, si $\frac{\mathfrak{A}}{\mathfrak{C}}$ fuera $= \frac{\alpha^m}{\gamma^m}$ entonces $\frac{\mathfrak{B}}{\mathfrak{D}}$ sería $= \frac{\alpha^{m+1}}{\gamma^{m+1}}$. En el artículo precedente mostramos que las cantidades $\frac{\alpha'}{\gamma'}$, $\frac{\alpha''}{\gamma''}$, $\frac{\alpha'''}{\gamma'''}$, etc. (a las que por brevedad denotaremos por (1), (2), (3), etc.) y L sigue este orden (I): (1), (3), (5), ... L, ... (6), (4), (2). La primera de estas cantidades es $= 0$ (puesto que $\alpha' = 0$); el resto tiene el mismo signo de L o a. Pero, puesto que por hipótesis $\frac{\mathfrak{A}}{\mathfrak{C}}$ y $\frac{\mathfrak{B}}{\mathfrak{D}}$ (para los cuales escribimos $\mathfrak{M}$ y $\mathfrak{N}$) tienen el mismo signo, es claro que estas cantidades están a la derecha de (1) (o si se prefiere en el mismo lado que L) y, de hecho, puesto que L está entre ellas, una está a la derecha de L, la otra a la izquierda. Con facilidad, puede mostrarse que $\mathfrak{M}$ no puede estar a la derecha de (2), pues de otra manera $\mathfrak{N}$ estaría entre (1) y L, de donde resultaría *primero* que (2) está entre $\mathfrak{M}$ y $\mathfrak{N}$, y el denominador de la fracción (2) sería mayor que el denominador de la fracción $\mathfrak{N}$ (art. 190); *segundo* que $\mathfrak{N}$ estaría entre (1) y (2) y el denominador de la fracción $\mathfrak{N}$ sería mayor que el denominador de la fracción (2), *Q. E. A.*

Supongamos que $\mathfrak{M}$ no es igual a ninguna de las fracciones (2), (3), (4), etc. Veamos lo que sucede. Si la fracción $\mathfrak{M}$ está a la izquierda de L, estará necesariamente entre (1) y (3), o entre (3) y (5), o entre (5) y (7), etc. (porque L es irracional, y entonces ciertamente no igual a $\mathfrak{M}$, las fracciones (1), (3), (5), etc. pueden aproximarse más a L que a cualquier cantidad dada diferente a L). Ahora, si $\mathfrak{M}$ está a la derecha de L, estará necesariamente entre (2) y (4), o entre (4) y (6), o entre (6) y (8), etc. Supongamos entonces que $\mathfrak{M}$ está entre (m) y $(m+2)$; es obvio que las cantidades $\mathfrak{M}$, (m), $(m+1)$, $(m+2)$, L están en el siguiente orden

$$(\text{II})^*): \quad (m),\ \mathfrak{M},\ (m+2),\ L,\ (m+1).$$

Entonces, necesariamente, $\mathfrak{N} = (m+1)$. Ahora $\mathfrak{N}$ estará a la derecha de L; pero si también está a la derecha de $(m+1)$, $(m+1)$ estará entre $\mathfrak{M}$ y $\mathfrak{N}$, de donde $\gamma^{m+1} > \mathfrak{C}$, y $\mathfrak{M}$ estará entre (m) y $(m+1)$, y por tanto $C > \gamma^{m+1}$ (art. 190), *Q. E. A.* Pero si $\mathfrak{N}$ estuviera a la izquierda de $(m+1)$, es decir entre $(m+2)$ y $(m+1)$, tendríamos $D > \gamma^{m+2}$, y puesto que $(m+2)$ está entre $\mathfrak{M}$ y $\mathfrak{N}$, tendríamos $\gamma^{m+2} > \mathfrak{D}$, *Q. E. A.* Tenemos, por lo tanto , $\mathfrak{N} = (m+1)$; es decir $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\alpha^{m+1}}{\gamma^{m+1}} = \frac{\beta^m}{\delta^m}$.

Puesto que $\mathfrak{AD} - \mathfrak{BC} = 1$, $\mathfrak{B}$ será primo con $\mathfrak{D}$, y por razón similar β^m será primo con δ^m. Entonces, se ve que la ecuación $\frac{\mathfrak{B}}{\mathfrak{D}} = \frac{\beta^m}{\delta^m}$ no puede ser consistente a menos que $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$ o $\mathfrak{B} = -\beta^m$, $\mathfrak{D} = -\delta^m$. Ahora, puesto que la forma f se transforma por la sustitución propia α^m, β^m, γ^m, δ^m en la forma f^m, que es $(\pm a^m, b^m, \mp a^{m+1})$, tendremos las ecuaciones

$$a\alpha^{2m} + 2b\alpha^m\gamma^m - a'\gamma^{2m} = \pm a^m \quad [5]$$

$$a\alpha^m\beta^m + b(\alpha^m\delta^m + \beta^m\gamma^m) - a'\gamma^m\delta^m = b^m \quad [6]$$

$$a\beta^{2m} + 2b\beta^m\delta^m - a'\delta^{2m} = \mp a^{m+1} \quad [7]$$

$$\alpha^m\delta^m - \beta^m\gamma^m = 1 \quad [8]$$

De aquí resulta (de las ecuaciones [7] y [3]): $\mp a^{m+1} = -A'$. Adicionalmente, al multiplicar la ecuación [2] por $\alpha^m\delta^m - \beta^m\gamma^m$, la ecuación [6] por $\mathfrak{AD} - \mathfrak{BC}$ y al restar obtenemos por un cálculo fácil que:

$$\begin{aligned} B - b^m = {} & (\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}\beta^m + b(\mathfrak{D}\beta^m + \mathfrak{B}\delta^m) - a'\mathfrak{D}\delta^m) \\ & + (\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)(a\mathfrak{A}\alpha^m + b(\mathfrak{C}\alpha^m + \mathfrak{A}\gamma^m) - a'\mathfrak{C}\gamma^m) \end{aligned} \quad [9]$$

*) No importa que el orden en (II) sea el mismo que en (I), u opuesto a él, i.e. que en (I) (m) esté a la izquierda de L o a la derecha de él.

o puesto que $\beta^m = \mathfrak{B}$, $\delta^m = \mathfrak{D}$ o $\beta^m = -\mathfrak{B}$, $\delta^m = -\mathfrak{D}$

$$B - b^m = \pm(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)(a\mathfrak{B}^2 + 2b\mathfrak{B}\mathfrak{D} - a'\mathfrak{D}^2) = \mp(\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m)A'$$

Entonces $B \equiv b^m \pmod{A'}$; y puesto que tanto B como b^m están entre $\sqrt{D}$ y $\sqrt{D} \mp A'$ tendremos $B = b^m$, y así $\mathfrak{C}\alpha^m - \mathfrak{A}\gamma^m = 0$ o $\frac{\mathfrak{A}}{\mathfrak{C}} = \frac{\alpha^m}{\gamma^m}$; i.e., $\mathfrak{M} = (m)$.

De esta forma, entonces, dedujimos de la suposición que $\mathfrak{M}$ no es igual a ninguna de las cantidades (2), (3), (4), etc., que de hecho es igual a alguna de ellas. Pero, si suponemos desde el principio que $\mathfrak{M} = (m)$, tendremos claramente $\mathfrak{A} = \alpha^m$, $\mathfrak{C} = \gamma^m$ o $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$. En cualquier caso, resulta de [1] y [5] $A = \pm a^m$ y de [9] $B - b^m = \pm(\mathfrak{B}\delta^m - \mathfrak{D}\beta^m)A$ o $B \equiv b^m \pmod{A}$. De esto concluimos de la misma forma como arriba que $B = b^m$, y entonces $\mathfrak{B}\delta^m = \mathfrak{D}\beta^m$; por lo tanto, puesto que $\mathfrak{B}$ es primo con $\mathfrak{D}$ y β^m con δ^m, será entonces $\mathfrak{B} = \beta^m$, $\mathfrak{D} = \delta^m$ o $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = \delta^m$, y de [7] $-A' = \mp a^{m+1}$. Entonces las formas F y f^m serán idénticas. Con la ayuda de la ecuación $\mathfrak{A}\mathfrak{D} - \mathfrak{B}\mathfrak{C} = \alpha^m\delta^m - \beta^m\gamma^m$ no es difícil mostrar que, cuando $+\mathfrak{A} = \alpha^m$, $+\mathfrak{C} = \gamma^m$ debe ponerse $+\mathfrak{B} = \beta^m$, $+\mathfrak{D} = \delta^m$; y por el otro lado, cuando $-\mathfrak{A} = \alpha^m$, $-\mathfrak{C} = \gamma^m$ debe ponerse $-\mathfrak{B} = \beta^m$, $-\mathfrak{D} = \delta^m$. *Q. E. D.*

III. Si el signo de las cantidades $\frac{\mathfrak{A}}{\mathfrak{C}}$ etc. es opuesto al de a, la demostración es tan similar a la precedente que es suficiente añadir solamente los puntos principales. La cantidad $\frac{-\sqrt{D}+b}{a'}$ estará entre $\frac{\mathfrak{C}}{\mathfrak{A}}$ y $\frac{\mathfrak{D}}{\mathfrak{B}}$. La fracción $\frac{\mathfrak{D}}{\mathfrak{B}}$ será igual a una de las fracciones

$$\frac{'\delta}{'\beta}, \quad \frac{''\delta}{''\beta}, \quad \frac{'''\delta}{'''\beta}, \quad \text{etc.} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(I)}$$

y si se pone ésta $= \frac{{}^m\delta}{{}^m\beta}$, $\qquad \frac{\mathfrak{C}}{\mathfrak{A}}$ será $= \frac{{}^m\gamma}{{}^m\alpha} \ldots\ldots\ldots\ldots\ldots\ldots$ (II)

Se demuestra (I) como sigue: si suponemos que $\frac{\mathfrak{D}}{\mathfrak{B}}$ no es igual a ninguna de estas fracciones, deberá caer entre dos de ellas $\frac{{}^m\delta}{{}^m\beta}$ y $\frac{{}^{m+2}\delta}{{}^{m+2}\beta}$. De donde, de la misma manera como se deduce arriba, mostramos que

$$\frac{\mathfrak{C}}{\mathfrak{A}} = \frac{{}^{m+1}\delta}{{}^{m+1}\beta} = \frac{{}^m\gamma}{{}^m\alpha}$$

y, o bien $\mathfrak{A} = {}^m\alpha$, $\mathfrak{C} = {}^m\gamma$ o bien $-\mathfrak{A} = {}^m\alpha$, $-\mathfrak{C} = {}^m\gamma$. Pero puesto que por la sustitución propia ${}^m\alpha$, ${}^m\beta$, ${}^m\gamma$, ${}^m\delta$ se transforma f en la forma

$${}^m f = (\pm {}^m a, {}^m b, \mp {}^{m-1} a)$$

podemos derivar tres ecuaciones. De éstas y de las ecuaciones [1], [2], [3], [4] y la ecuación ${}^m\alpha{}^m\delta - {}^m\beta{}^m\gamma = 1$ deducimos de la misma manera que arriba que el primer término A de la forma F es igual al primer término de la forma ${}^m f$ y que el término del medio de la anterior es congruente (según el módulo A) al término del medio del último. Puesto que ambas formas son reducidas, el término del medio de cada una está entre $\sqrt{D}$ y $\sqrt{D} \mp A$, y entonces estos términos del medio serán iguales. De esto concluimos que $\frac{{}^m\delta}{{}^m\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$. La veracidad de la afirmación (I) es derivada suponiendo que esto es falso.

Supóngase que $\frac{{}^m\delta}{{}^m\beta} = \frac{\mathfrak{D}}{\mathfrak{B}}$. De la misma forma y usando las mismas ecuaciones, podemos mostrar que $\frac{{}^m\gamma}{{}^m\alpha} = \frac{\mathfrak{C}}{\mathfrak{A}}$, que era la segunda afirmación (II). Ahora, con la ayuda de las ecuaciones $\mathfrak{AD} - \mathfrak{BC} = 1$, ${}^m\alpha{}^m\delta - {}^m\beta{}^m\gamma = 1$ deducimos que o bien

$$\mathfrak{A} = {}^m\alpha, \quad \mathfrak{B} = {}^m\beta, \quad \mathfrak{C} = {}^m\gamma, \quad \mathfrak{D} = {}^m\delta$$

o bien

$$-\mathfrak{A} = {}^m\alpha, \quad -\mathfrak{B} = {}^m\beta, \quad -\mathfrak{C} = {}^m\gamma, \quad -\mathfrak{D} = {}^m\delta$$

y las formas F y ${}^m f$ son idénticas. *Q. E. D.*

194.

Puesto que las formas que arriba hemos llamado asociadas (art. 187.6) son siempre impropiamente equivalentes (art. 159), es claro que si las formas reducidas F y f son impropiamente equivalentes, y si la forma G es la asociada de la forma F, entonces las formas f y G serán propiamente equivalentes y la forma G estará contenida en el período de la forma f. Y si las formas F y f son equivalentes tanto propiamente como impropiamente, es claro que ambas F y G deberán ser encontradas en el período de la forma f. Por lo tanto, este período será un asociado de él mismo y contendrá dos formas ambiguas (art. 187.7). Entonces, se confirma perfectamente el teorema del artículo 165, ya garantizado, que podemos encontrar una forma ambigua equivalente a las formas F y f.

195.

PROBLEMA. *Dadas dos formas cualesquiera* Φ *y* φ *del mismo determinante, determinar cuándo son o no equivalentes.*

Solución. Búsquense dos formas reducidas F y f propiamente equivalentes a las formas dadas Φ y φ (art. 183). Ahora, según que éstos sean sólo propiamente equivalentes o sólo impropiamente equivalentes o ambas o ninguna, entonces las formas dadas serán sólo propiamente equivalentes, o sólo impropiamente, o ambas o ninguna. Se calcula el período de una de las formas reducidas, e.g., el período de la forma f. Si la forma F aparece en este período aunque no la forma de su asociada, entonces tendrá lugar el *primer* caso; por otro lado, si la asociada aparece aquí pero F no, ocurre el *segundo* caso; si ambas aparecen, se da el *tercer* caso; si ninguna aparece, se da el *cuarto* caso.

Ejemplo. Sean las formas dadas $(129, 92, 65)$ y $(42, 59, 81)$ con determinante 79. Para éstas tenemos las formas reducidas propiamente equivalentes $(10, 7, -3)$ y $(5, 8, -3)$. El período de la primera de éstas es : $(10, 7, -3)$, $(-3, 8, 5)$, $(5, 7, -6)$, $(-6, 5, 9)$, $(9, 4, -7)$, $(-7, 3, 10)$. Puesto que la forma $(5, 8, -3)$ no aparece aquí sino sólo su asociada $(-3, 8, 5)$, concluimos que las formas dadas son sólo impropiamente equivalentes.

Si todas las formas reducidas de un determinante dado son distribuidas de la misma forma que arriba (art. 187.5) en períodos P, Q, R, etc., y si se selecciona una forma de cada período al azar, F de P; G de Q; H de R, etc., entonces ningún par de las formas F, G, H, etc. podrán ser propiamente equivalentes. Y cualquier otra forma del mismo determinante será propiamente equivalente a una y *solo una* de éstas. Entonces, *todas las formas de este determinante pueden ser distribuidas en tantas clases como períodos tenga,* esto es: poniendo las formas que son propiamente equivalentes a la forma F en la primera clase, aquéllas que son propiamente equivalentes a G en la segunda clase, etc. De esta manera, todas las formas contenidas en la misma clase serán propiamente equivalentes, y las formas contenidas en clases diferentes no pueden ser propiamente equivalentes. Pero no nos detendremos aquí en este tema que será tratado en detalle más adelante.

196.

PROBLEMA. *Dadas dos formas propiamente equivalentes Φ y φ: encontrar una transformación propia de una en la otra.*

Solución. Por el método del artículo 183 podrán encontrarse dos series de formas

$$\Phi,\ \Phi',\ \Phi'',\ \ldots \Phi^n \qquad \text{y} \qquad \varphi,\ \varphi',\ \varphi'',\ \ldots \varphi^v$$

tales que cada forma equivalga propiamente a su predecesora y las últimas Φ^n y φ^v sean formas reducidas. Y, puesto que supusimos que Φ y φ eran propiamente equivalentes, Φ^n estará necesariamente contenida en el período de la forma φ^v. Sea $\varphi^v = f$ y sea su período hasta la forma Φ^n :

$$f,\ f',\ f'',\ \ldots f^{m-1},\ \Phi^n$$

tal que en este período el índice de la forma Φ^n sea m; y se designarán las formas que son opuestas a las asociadas de las formas

$$\Phi,\ \Phi',\ \Phi'',\ \ldots \Phi^n \quad \text{por} \quad \Psi,\ \Psi',\ \Psi'',\ \ldots \Psi^n \quad \text{respectivamente*)}$$

Entonces en la sucesión

$$\varphi,\ \varphi',\ \varphi'',\ \ldots, f,\ f',\ f'',\ \ldots f^{m-1},\ \Psi^{n-1},\ \Psi^{n-2},\ \ldots \Psi,\ \Phi$$

cada forma será contigua a la precedente por la última parte, y por el artículo 177 podemos obtener una transformación propia de la primera φ en la última Φ. Esto es fácil de ver para los otros términos de la sucesión; para los términos f^{m-1} y Ψ^{n-1} lo probamos como sigue: sea

$$f^{m-1} = (g, h, i); \qquad f^m \quad \text{o} \quad \Phi^n = (g', h', i'); \qquad \Phi^{n-1} = (g'', h'', i'')$$

La forma (g', h', i') será contigua por la última parte de cada una de las formas (g, h, i) y (g'', h'', i''); por lo tanto, $i = g' = i''$ y $-h \equiv h' \equiv -h''$ (mod. i o g' o i''). De esto, es manifiesto que la forma $(i'', -h'', g'')$, i.e., la forma Ψ^{n-1} es contigua por la última parte de la forma (g, h, i), i.e., de la forma f^{m-1}.

Si las formas Φ y φ son impropiamente equivalentes, la forma φ equivaldrá propiamente a la forma opuesta a Φ. Podemos, entonces, encontrar la transformación propia de la forma φ en la forma opuesta a Φ; si suponemos que esto puede darse por la sustitución α, β, γ, δ, es fácil ver que φ se transformará impropiamente en Φ por la sustitución α, $-\beta$, γ, $-\delta$.

De aquí es claro que si las formas Φ y φ son propia e impropiamente equivalentes, podemos encontrar *dos* transformaciones, una propia y la otra impropia.

*) Ψ se deriva de Φ intercambiando el primer y el último términos y asignando el signo opuesto al término del medio. Lo mismo vale para los otros miembros de la serie.

Ejemplo. Se busca una transformación impropia de la forma $(129, 92, 65)$ en la forma $(42, 59, 81)$, ya que observamos en el artículo anterior que las dos formas son impropiamente equivalentes. Se deberá primero encontrar una transformación propia de la forma $(129, 92, 65)$ en la forma $(42, -59, 81)$. Para este fin, calculamos la sucesión de formas $(129, 92, 65)$, $(65, -27, 10)$, $(10, 7, -3)$, $(-3, 8, 5)$, $(5, 22, 81)$, $(81, 59, 42)$, $(42, -59, 81)$. De esta se deduce la transformación propia -47, 56, 73, -87, a través de la cual $(129, 92, 65)$ se transforma en $(42, -59, 81)$; por lo tanto se transformará en $(42, 59, 81)$ por la transformación impropia -47, -56, 73, 87.

197.

Si tenemos una transformación de una forma $(a, b, c) \ldots \varphi$ en una forma equivalente Φ, de esto podrán deducirse *todas* las transformaciones similares de la forma φ en Φ, si solamente podemos determinar todas las soluciones de la ecuación indeterminada $t^2 - Du^2 = m^2$, donde D indica el determinante de las formas Φ y φ, m es el máximo común divisor de los números a, $2b$, c (art. 162). Solucionamos este problema arriba para un valor negativo de D, y ahora consideraremos un valor positivo. Pero, puesto que obviamente cualquier valor de t o u que satisfaga la ecuación también la satisfará si cambiamos el signo, será suficiente asignar valores *positivos* a t y a u. De hecho, cualquier solución por valores positivos proporcionará cuatro soluciones efectivas. Para resolver este asunto, encontraremos primero los valores *mínimos* de t y u (excepto aquéllos obvios donde $t = m$ y $u = 0$) y entonces de éstos veremos cómo derivar los otros.

198.

PROBLEMA. *Encontrar los números menores t y u que satisfacen la ecuación indeterminada $t^2 - Du^2 = m^2$ si se da alguna forma (M, N, P) cuyo determinante es D y si m es el máximo común divisor de M, $2N$ y P.*

Solución. Tomemos a voluntad la forma reducida $(a, b, -a') \ldots f$ con determinante D, en la cual el máximo común divisor de los números a, $2b$, a' sea m. Es claro de ahí que ésa existe porque puede encontrarse una forma reducida equivalente a la forma (M, N, P), la cual por el artículo 161 está dotada con esta propiedad. Pero para nuestro presente propósito, cualquier forma reducida que satisface esta condición puede ser usada. Calculemos el período de la forma f, el cual supondremos consiste de n formas. Reteniendo la notación que hemos usado en el artículo

188, f^n será $(+a^n, b^n, -a^{n+1})$ porque n es par y f será transformada en esta forma por la sustitución propia α^n, β^n, γ^n, δ^n. Pero, puesto que f y f^n son idénticas, f se transformará en f^n también por la sustitución propia 1, 0, 0, 1. De estas dos transformaciones similares de la forma f en f^n, por el artículo 162 podrá deducirse una solución *integral* de la ecuación $t^2 - Du^2 = m^2$, a saber $t = \frac{1}{2}(\alpha^n + \delta^n)m$ (ecuación 18, art. 162), $u = \frac{\gamma^n m}{a}$ (ecuación 19).*) Tómense estos valores positivamente si no lo son ya y desígnense por T y U. Estos valores T y U serán los valores menores de t y u excepto $t = m$ y $u = 0$ (ellos deben ser diferentes de estos, puesto que claramente γ^n no podría ser $= 0$).

Supóngase en efecto que hay valores menores de t y u, llamados $\mathfrak{t}$ y $\mathfrak{u}$, los cuales son positivos y $\mathfrak{u}$ no es $= 0$. Entonces por el artículo 162 la forma f se transformará en una forma que es idéntica a ella misma por la transformación propia $\frac{1}{m}(\mathfrak{t}-b\mathfrak{u})$, $\frac{1}{m}a'\mathfrak{u}$, $\frac{1}{m}a\mathfrak{u}$, $\frac{1}{m}(\mathfrak{t}+b\mathfrak{u})$. Ahora, por el artículo 193, II resulta que *o* $\frac{1}{m}(\mathfrak{t}-b\mathfrak{u})$ *o bien* $-\frac{1}{m}(\mathfrak{t}-b\mathfrak{u})$ debe ser igual a uno de los números α'', α''', α'''', etc., por ejemplo a α^μ (puesto que $\mathfrak{t}^2 = D\mathfrak{u}^2 + m^2 = b^2\mathfrak{u}^2 + aa'\mathfrak{u}^2 + m^2$ tenemos $\mathfrak{t}^2 > b^2\mathfrak{u}^2$ y por lo tanto $\mathfrak{t} - b\mathfrak{u}$ es positivo; de aqui la fracción $\frac{\mathfrak{t}-b\mathfrak{u}}{a\mathfrak{u}}$ que corresponde a la fracción $\frac{\mathfrak{A}}{\mathfrak{C}}$ en el artículo 193 tendrá el mismo signo que a o a'); y en el primer caso $\frac{1}{m}a'\mathfrak{u}$, $\frac{1}{m}a\mathfrak{u}$, $\frac{1}{m}(\mathfrak{t}+b\mathfrak{u})$ serán iguales a β^μ, γ^μ, δ^μ respectivamente, y en el último caso serán iguales a las mismas cantidades pero con cambio de signo. Puesto que $\mathfrak{u} < U$, i.e. $\mathfrak{u} < \frac{\gamma^n m}{a}$ y > 0, obtenemos $\gamma^\mu < \gamma^n$ y > 0; y puesto que la sucesión γ, γ', γ'', etc., es continuamente creciente, μ estará necesariamente entre 0 y n exclusivamente. Así la forma correspondiente f^μ será idéntica a la forma f, *Q. E. A.* puesto que todas las formas f, f', f'', etc., hasta f^{n-1} se suponen diferentes. De esto concluimos que los valores menores de t y u (excepto los valores m y 0) serán T y U.

Ejemplo. Si $D = 79$ y $m = 1$ podemos usar la forma $(3, 8, -5)$ para la cual $n = 6$, y $\alpha^n = -8$, $\gamma^n = -27$, $\delta^n = -152$ (art. 188). Entonces $T = 80$ y $U = 9$, que son los valores menores de los números t y u, que satisfacen la ecuación $t^2 - 79u^2 = 1$.

199.

En la práctica, pueden desarrollarse fórmulas aún más cómodas. Tenemos $2b\gamma^n = -a(\alpha^n - \delta^n)$, que es fácil de deducir del artículo 162, multiplicando la ecuación [19] por $2b$, [20] por a, y cambiando los símbolos usados allí por los que

*) Las cantidades que en el artículo 162 eran $\alpha,\beta,\gamma,\delta$; $\alpha', \beta', \gamma', \delta'$; $A,B,\ C$; $a,b,\ c$; e,
aquí son $1,0,0,1$; $\alpha^n,\beta^n,\gamma^n,\delta^n$; $a,\ b,-a'$; $a,b,-a'$; 1.

estamos usando aquí. De esto obtenemos $\alpha^n + \delta^n = 2\delta^n - \frac{2b}{a}\gamma^n$ y entonces

$$\pm T = m(\delta^n - \frac{b}{a}\gamma^n), \qquad \pm U = \frac{\gamma^n m}{a}$$

Por un método similar obtendremos los valores siguientes

$$\pm T = m(\alpha^n + \frac{b}{a'}\beta^n), \qquad \pm U = \frac{\beta^n m}{a'}$$

Estos dos conjuntos de fórmulas son muy convenientes porque $\gamma^n = \delta^{n-1}$ y $\alpha^n = \beta^{n-1}$, de modo que si usamos el segundo conjunto, es suficiente calcular la sucesión β', β'', β''', ..., β^n; y si usamos el primer conjunto, la sucesión δ', δ'', δ''', etc., será suficiente. Más aún, del artículo 189.3 podemos fácilmente deducir que, puesto que n es par, α^n y $\frac{b}{a'}\beta^n$ tienen el mismo signo. Esto es también cierto para δ^n y $\frac{b}{a}\gamma^n$, de modo que en la primera fórmula deba tomarse para T la diferencia absoluta, y en la segunda la suma absoluta sin que sea necesario prestar atención al signo. Usando los símbolos del artículo 189.4 obtenemos de la primera fórmula lo siguiente:

$$T = m[k', k'', k''', \ldots k^n] - \frac{mb}{a}[k', k'', k''', \ldots k^{n-1}], \qquad U = \frac{m}{a}[k', k'', k''', \ldots k^{n-1}]$$

y de la segunda fórmula resulta:

$$T = m[k'', k''', \ldots k^{n-1}] + \frac{mb}{a'}[k'', k''', \ldots k^n], \qquad U = \frac{m}{a'}[k'', k''', \ldots k^n]$$

donde podemos también escribir $m[k'', k''', \ldots k^n, \frac{b}{a'}]$ para el valor de T.

Ejemplo. Para $D = 61$, $m = 2$, puede usarse la forma $(2, 7, -6)$. De esto encontramos $n = 6$; k', k'', k''', k'''', k''''', k'''''' respectivamente $= 2, 2, 7, 2, 2, 7$. Entonces

$$T = 2[2, 2, 7, 2, 2, 7] - 7[2, 2, 7, 2, 2] = 2888 - 1365 = 1523$$

de la primera fórmula; lo mismo resulta de la segunda fórmula

$$T = 2[2, 7, 2, 2] + \frac{7}{3}[2, 7, 2, 2, 7]$$

y

$$U = [2, 2, 7, 2, 2] = \frac{1}{3}[2, 7, 2, 2, 7] = 195.$$

Existen otros artificios mediante los cuales puede simplificarse el cálculo, pero la brevedad no nos permite tratarlos en detalle aquí.

200.

Para obtener *todos* los valores de t y u de los valores menores, presentaremos la ecuación $T^2 - DU^2 = m^2$ de la siguiente forma

$$(\frac{T}{m} + \frac{U}{m}\sqrt{D})(\frac{T}{m} - \frac{U}{m}\sqrt{D}) = 1$$

De esto tenemos también que

$$(\frac{T}{m} + \frac{U}{m}\sqrt{D})^e(\frac{T}{m} - \frac{U}{m}\sqrt{D})^e = 1 \qquad [1]$$

donde e puede ser cualquier número. Ahora por brevedad designaremos los valores de las cantidades

$$\frac{m}{2}(\frac{T}{m} + \frac{U}{m}\sqrt{D})^e + \frac{m}{2}(\frac{T}{m} - \frac{U}{m}\sqrt{D})^e$$
$$\frac{m}{2\sqrt{D}}(\frac{T}{m} + \frac{U}{m}\sqrt{D})^e - \frac{m}{2\sqrt{D}}(\frac{T}{m} - \frac{U}{m}\sqrt{D})^e \text{ *)}$$

en general por t^e y u^e, respectivamente; i.e., para $e = 0$ serán t^0 y u^0 (estos valores son m y 0); para $e = 1$ será t' y u' (estos valores son T y U); para $e = 2$ serán t'' y u''; para $e = 3$ serán t''' y u''', etc. Además mostraremos que, si para e se toman todos los enteros no negativos, i.e., 0 y todos los enteros positivos de 1 a ∞, estas expresiones producirán todos los valores positivos de t y u; es decir, (I) todos los valores de estas expresiones son, en efecto, valores de t y u; (II) todos estos valores son enteros; (III) no existen valores positivos de t y u que no estén contenidos en estas fórmulas.

I. Si sustituimos t^e y u^e por sus valores y usamos la ecuación [1] es fácil encontrar que

$$(t^e + u^e\sqrt{D})(t^e - u^e\sqrt{D}) = m^2, \qquad \text{i.e.} \quad t^{2e} - Du^{2e} = m^2$$

II. De la misma forma es fácil confirmar que en general

$$t^{e+1} + t^{e-1} = \frac{2T}{m}t^e, \qquad u^{e+1} + u^{e-1} = \frac{2T}{m}u^e$$

*) Solamente en estas cuatro expresiones y en la ecuación [1] e denota el *exponente* de la potencia; en las restantes las letras escritas arriba siempre designan el *índice*.

Entonces, es claro que las dos sucesiones t^0, t', t'', t''', etc., u^0, u', u'', u''', etc. son recurrentes y que los factores correspondientes para cada una son $\frac{2T}{m}$ y -1, es decir

$$t'' = \frac{2T}{m}t' - t^0, \qquad t''' = \frac{2T}{m}t'' - t' \text{ etc.}, \qquad u'' = \frac{2T}{m}u' \text{ etc.}$$

Ahora, puesto que por hipótesis tenemos una forma (M, N, P) con determinante D en la cual M, $2N$, P son divisibles por m, tendremos

$$T^2 = (N^2 - MP)U^2 + m^2$$

y manifiestamente $4T^2$ será divisible por m^2. Entonces $\frac{2T}{m}$ será un entero positivo. Y puesto que $t^0 = m$, $t' = T$, $u^0 = 0$, $u' = U$, y son entonces enteros, todos los números t'', t''', etc., u'', u''', etc., serán también enteros. Más aún, puesto que $T^2 > m^2$, todos los números t^0, t', t'', t''', etc. serán positivos y continuamente crecientes al infinito; lo mismo es cierto para los números u^0, u', u'', u''', etc.

III. Supongamos que existen otros valores positivos de t y u, no contenidos en la serie t^0, t', t'', etc. u^0, u', u'', etc., llamados $\mathfrak{T}$ y $\mathfrak{U}$. Puesto que la serie u^0, u', etc. crece de 0 a infinito, $\mathfrak{U}$ estará necesariamente entre dos términos vecinos u^n y u^{n+1} tal que $\mathfrak{U} > u^n$ y $\mathfrak{U} < u^{n+1}$. Para mostrar lo absurdo de esta suposición, observamos que

1^o La ecuación $t^2 - Du^2 = m^2$ se satisface si se ponen

$$t = \frac{1}{m}(\mathfrak{T}t^n - D\mathfrak{U}u^n), \qquad u = \frac{1}{m}(\mathfrak{U}t^n - \mathfrak{T}u^n)$$

Esto puede confirmarse sin dificultad por sustitución. Así mostraremos que estos valores, que por brevedad escribimos τ y ν, son siempre *enteros*. Si (M, N, P) es una forma con determinante D y m es el máximo común divisor de los números M, $2N$, P, ambos $\mathfrak{T} + N\mathfrak{U}$ y $t^n + Nu^n$ serán divisibles por m y por lo tanto también $\mathfrak{U}(t^n + Nu^n) - u^n(\mathfrak{T} + N\mathfrak{U})$ o $\mathfrak{U}t^n - \mathfrak{T}u^n$. Por esto ν será un entero y también lo será τ porque $\tau^2 = D\nu^2 + m^2$.

2^o Claramente ν no puede ser $= 0$; puesto que de esto resultaría que

$$\mathfrak{U}^2 t^{2n} = \mathfrak{T}^2 u^{2n}$$

o

$$\mathfrak{U}^2(Du^{2n} + m^2) = u^{2n}(D\mathfrak{U}^2 + m^2)$$

o $\mathfrak{U}^2 = u^{2n}$ en contra de la hipótesis de que $\mathfrak{U} > u^n$. Puesto que excepto para el valor 0, el valor menor de u es U, ν ciertamente no será menor que U.

3^o De los valores de t^n, t^{n+1}, u^n, u^{n+1} es fácil confirmar que

$$mU = u^{n+1}t^n - t^{n+1}u^n$$

Y así $\mathfrak{U}t^n - \mathfrak{T}u^n$ ciertamente no será menor que $u^{n+1}t^n - t^{n+1}u^n$.

4^o Ahora, de la ecuación $\mathfrak{T}^2 - D\mathfrak{U}^2 = m^2$ tenemos

$$\frac{\mathfrak{T}}{\mathfrak{U}} = \sqrt{D + \frac{m^2}{\mathfrak{U}^2}}$$

y similarmente

$$\frac{t^{n+1}}{u^{n+1}} = \sqrt{D + \frac{m^2}{u^{2n+2}}}$$

De esto es fácil de ver que $\frac{\mathfrak{T}}{\mathfrak{U}} > \frac{t^{n+1}}{u^{n+1}}$. Esto, a la par de la conclusión en 3^o, nos da

$$(\mathfrak{U}t^n - \mathfrak{T}u^n)(t^n + u^n\frac{\mathfrak{T}}{\mathfrak{U}}) > (u^{n+1}t^n - t^{n+1}u^n)(t^n + u^n\frac{t^{n+1}}{u^{n+1}})$$

Si se multiplican y en lugar de $\mathfrak{T}^2$, t^{2n}, t^{2n+2} se sustituyen sus valores $D\mathfrak{U}^2 + m^2$, $Du^{2n} + m^2$, $Du^{2n+2} + m^2$, resultará que

$$\frac{1}{\mathfrak{U}}(\mathfrak{U}^2 - u^{2n}) > \frac{1}{u^{n+1}}(u^{2n+2} - u^{2n})$$

De esto, puesto que cada cantidad es positiva, resultará trasponiendo $\mathfrak{U} + \frac{u^{2n}}{u^{n+1}} > u^{n+1} + \frac{u^{2n}}{\mathfrak{U}}$, *Q. E. A.* ; porque la primera parte de la primera cantidad es *menor* que la primera parte de la segunda cantidad y la segunda parte de la primera es menor que la segunda parte de la última. Por lo tanto la suposición es inconsistente y las sucesiones t^0, t', t'', etc., u^0, u', u'', etc., exhibirán todos los valores posibles de t y u.

Ejemplo. Para $D = 61$ y $m = 2$ encontramos que los valores positivos menores de t y u, son 1523 y 195, así pues *todos* los valores positivos serán expresados por la fórmula

$$t = (\frac{1523}{2} + \frac{195}{2}\sqrt{61})^e + (\frac{1523}{2} - \frac{195}{2}\sqrt{61})^e$$
$$u = \frac{1}{\sqrt{61}}((\frac{1523}{2} + \frac{195}{2}\sqrt{61})^e - (\frac{1523}{2} - \frac{195}{2}\sqrt{61})^e)$$

Además se encuentra que
$t^0 = 2$, $t' = 1523$, $t'' = 1523t' - t^0 = 2319527$, $t''' = 1523t'' - t' = 3532638098$, etc.
$u^0 = 0$, $u' = 195$, $u'' = 1523u' - u^0 = 296985$, $u''' = 1523u'' - u' = 452307960$, etc.

201.

Añadimos las siguientes observaciones acerca del problema tratado en los artículos precedentes.

1) Puesto que hemos mostrado cómo resolver la ecuación $t^2 - Du^2 = m^2$ para todos los casos cuando m es el máximo común divisor de los tres números M, $2N$, P, tal que $N^2 - MP = D$, es útil especificar todos los números que pueden ser esos divisores, es decir, todos los valores de m para un valor dado de D. Sea $D = n^2 D'$ de modo que D' esté enteramente libre de factores cuadrados. Esto puede obtenerse poniendo n^2 como el cuadrado mayor que divide D y, si D no tiene un factor cuadrado, poniendo $n = 1$. Entonces:

Primero, si D' es de la forma $4k + 1$, cualquier divisor de $2n$ será un valor de m y viceversa. En efecto, si g es un divisor de $2n$, tendremos la forma $(g, n, \frac{n^2(1-D')}{g})$, cuyo determinante es D y en la cual el máximo común divisor de los números g, $2n$, $\frac{n^2(D'-1)}{g}$ será obviamente g (puesto que es claro que $\frac{n^2(D'-1)}{g^2} = \frac{4n^2}{g^2} \cdot \frac{(D'-1)}{4}$ es un entero). Si, por el otro lado, suponemos que g es un valor de m, es decir, el máximo común divisor de los números M, $2N$, P, y que $N^2 - MP = D$, manifiestamente $4D$ o $4n^2 D'$ será divisible por g^2. Se sigue que $2n$ es divisible por g. Pues, si g no dividiera a $2n$, g y $2n$ tendrían un máximo común divisor menor que g. Supóngase que fuera $= \delta$, y $2n = \delta n'$, $g = \delta g'$; $n'^2 D'$ será divisible por g'^2. Así, n' y g' al igual que n'^2 y g'^2 serían primos relativos y D' sería divisible por g'^2, en contra de la hipótesis según la cual D' está libre de factores cuadrados.

Segundo, si D' es de la forma $4k + 2$ o $4k + 3$, cualquier divisor de n será un valor de m e, inversamente, cualquier valor de m dividirá n. En efecto, si g es un divisor de n se tendrá una forma $(g, 0, \frac{-n^2 D'}{g})$ cuyo determinante es $= D$. Claramente el máximo común divisor de los números $g, 0, \frac{n^2 D'}{g}$ será g. Ahora, si suponemos que g es un valor de m, es decir, el máximo común divisor de los números $M, 2N, P$ y que $N^2 - MP = D$, de la misma forma que arriba, g dividirá $2n$ y $\frac{2n}{g}$ será un entero. Si este cociente es impar, el cuadrado $\frac{4n^2}{g^2}$ será $\equiv 1 \pmod 4$, y entonces $\frac{4n^2 D'}{g^2}$ sería $\equiv 2$, o $\equiv 3 \pmod 4$. Pero $\frac{4n^2 D'}{g^2} = \frac{4D}{g^2} = \frac{4N^2}{g^2} - \frac{4MP}{g^2} \equiv \frac{4N^2}{g^2} \pmod 4$ y entonces $\frac{4n^2}{g^2}$ sería $\equiv 2$ o $\equiv 3 \pmod 4$, Q.E.A, porque todo cuadrado debe ser congruente a cero o a la unidad según el módulo 4. Por lo tanto, el cociente $\frac{2n}{g}$ será necesariamente par, y así $\frac{n}{g}$ es un entero, es decir, g un divisor de n.

Entonces es claro que 1 es siempre un valor de m, es decir, que la ecuación $t^2 - Du^2 = 1$ es resoluble de la manera precedente para cualquier valor no cuadrado

positivo de D; 2 será un valor de m sólo si D es de la forma $4k$ o $4k+1$.

2) Si m es mayor que 2 pero es todavía un número idóneo, la solución de la ecuación $t^2 - Du^2 = m^2$ puede reducirse a la solución de una ecuación similar en la cual m es 1 o 2. Así, poniendo $D = n^2 D'$, si m divide a n, m^2 dividirá a D. Entonces si suponemos que los valores menores de p y q en la ecuación $p^2 - \frac{D}{m^2}q^2 = 1$ son $p = P$ y $q = Q$, los valores menores de t y u en la ecuación $t^2 - Du^2 = m^2$ serán $t = mP$ y $u = Q$. Pero si m no divide a n, al menos dividirá a $2n$ y será ciertamente par, y $4D/m^2$ será un entero. Entonces, si se encuentra que los valores menores de p y q en la ecuación $p^2 - \frac{4D}{m^2}q^2 = 4$ son $p = P$ y $q = Q$, los valores menores de t y u en la ecuación $t^2 - Du^2 = m^2$ serán $t = \frac{m}{2}P$ y $u = Q$. En cualquier caso, sin embargo, podrán deducirse no sólo los valores menores de t y u por el conocimiento de los valores menores de p y q, sino que, por este método podrán deducirse *todos* los valores del anterior de *todos* los valores del último.

3) Designemos por t^0, u^0; t', u'; t'', u'', etc. a todos los valores positivos de t y u, en la ecuación $t^2 - Du^2 = m^2$ (como en el artículo precedente). Si resulta que cualesquiera valores en la serie son congruentes a los primeros valores según un módulo dado r, por ejemplo si $t^\rho \equiv t^0$ (o $\equiv m$), $u^\rho \equiv u^0$ o $\equiv 0 \pmod{r}$, y si al mismo tiempo los valores siguientes son congruentes a los segundos valores, i.e.,

$$t^{\rho+1} \equiv t', \qquad u^{\rho+1} \equiv u' \pmod{r}$$

se tendrá también que

$$t^{\rho+2} \equiv t'', \quad u^{\rho+2} \equiv u''; \qquad t^{\rho+3} \equiv t''', \quad u^{\rho+3} \equiv u'''; \text{ etc.}$$

Esto puede deducirse facilmente porque cada serie t^0, t', t'', etc., u^0, u', u'', etc. es una serie recurrente; esto es así puesto que

$$t'' = \frac{2T}{m}t' - t^0, \qquad t^{\rho+2} = \frac{2T}{m}t^{\rho+1} - t^\rho$$

será

$$t'' \equiv t^{\rho-2}$$

y similarmente para el resto. Entonces se sigue que en general

$$t^{h+\rho} \equiv t^h, \qquad u^{h+\rho} \equiv u^h \pmod{r}$$

donde h es cualquier número; e incluso, más generalmente, si

$$\mu \equiv \nu \pmod{\rho}, \qquad \text{entonces} \quad t^\mu \equiv t^\nu, \quad u^\mu \equiv u^\nu \pmod{r}$$

4) Podemos siempre satisfacer las condiciones requeridas por la observación precedente; esto es, siempre puede encontrarse un índice ρ (para cualquier módulo dado r) para el cual sean

$$t^\rho \equiv t^0, \quad t^{\rho+1} \equiv t', \quad u^\rho \equiv u^0, \quad u^{\rho+1} \equiv u'$$

Para mostrar esto, observamos:

Primero, que la tercera condición siempre puede satisfacerse. Pues por los criterios dados en 1) es claro que la ecuación $p^2 - r^2Dq^2 = m^2$ es resoluble, y si se supone que los valores positivos menores de p y q (excepto m y 0) son P y Q, manifiestamente $t = P$ y $u = rQ$ estará entre los valores de t y u. Por lo tanto P y rQ estarán contenidos en las sucesiones t^0, t', etc., u^0, u', etc., y si $P = t^\lambda$ y $rQ = u^\lambda$ tendremos $u^\lambda \equiv 0 \equiv u^0 \pmod{r}$. Más aún, se ve que entre u^0 y u^λ no existirá ningún término que sea congruente a u^0 según el módulo r.

Segundo, si las otras tres condiciones se cumplen, es decir, si $u^{\lambda+1} \equiv u'$, $t^\lambda \equiv t^0$, $t^{\lambda+1} \equiv t'$, entonces se debe poner $\rho = \lambda$. Pero, si una u otra de estas condiciones no se cumple, podemos con certeza poner $\rho = 2\lambda$. En efecto, de la ecuación [1] y las fórmulas generales para t^e y u^e del artículo precedente se deduce

$$t^{2\lambda} = \frac{1}{m}(t^{2\lambda} + Du^{2\lambda}) = \frac{1}{m}(m^2 + 2Du^{2\lambda})$$

y entonces

$$\frac{t^{2\lambda} - t^0}{r} = \frac{2Du^{2\lambda}}{mr}$$

Esta cantidad será un entero porque por hipótesis r divide a u^λ y m^2 divide a $4D$ y, así, m divide a $2D$. Más aún $u^{2\lambda} = \frac{2}{m}t^\lambda u^\lambda$, y puesto que

$$4t^{2\lambda} = 4Du^{2\lambda} + 4m^2$$

es entonces divisible por m^2, $2t^\lambda$ será divisible por m y entonces $u^{2\lambda}$ por r o

$$u^{2\lambda} \equiv u^0 \pmod{r}$$

En el tercer lugar se encuentra

$$t^{2\lambda+1} = t' + \frac{2Du^{2\lambda+1}}{m}$$

y puesto que, por una razón similar, $\frac{2Du^{\lambda}}{mr}$ es un entero, se tendrá

$$t^{2\lambda+1} \equiv t' \pmod{r}$$

Finalmente se encuentra que

$$u^{2\lambda+1} = u' + \frac{2t^{\lambda+1}u^{\lambda}}{m}$$

y puesto que $2t^{\lambda+1}$ es divisible por m y u^{λ} por r, tenemos que

$$u^{2\lambda+1} \equiv u' \pmod{r}. \quad Q.\ E.\ D.$$

La utilidad de las últimas dos observaciones aparecerá en lo siguiente.

202.

Un caso particular del problema de resolver la ecuación $t^2 - Du^2 = 1$ ya ha sido tratado por geómetras del último siglo. El extremadamente agudo geómetra Fermat propuso el problema a los analistas ingleses, y Wallis atribuyó el descubrimiento de la solución a Brounker, y reportó éste en el capítulo 98 de su *Algebra*, *Opera T.* II, *p.* 418 y siguientes. Ozanam afirma que fue Fermat; y Euler, que trató de él en *Comm. Petr. VI p.* 175, *Comm. nov. XI, p.* 28 *), *Algebra P.* 2, *p.* 226, *Opusc. An. I, p.* 310, afirma que Pell fue el descubridor, y por esa razón se llama el problema de Pell por algunos autores. Todas estas soluciones coinciden esencialmente con lo que obtenemos si en el artículo 198 usamos la forma reducida con $a = 1$; pero nadie antes de Lagrange mostró que la operación necesariamente termina, es decir que el

*) En este comentario el algoritmo que consideramos en el artículo 27 se presenta con una notación similar. No lo reconocimos así en aquel momento.

problema es *realmente resoluble**). Consúltese *Mélanges de la Soc. de Turin, T.* 4, *p.* 19; y para una presentación más elegante *Hist. de l'Ac. de Berlin*, 1767, *p.* 237. También hay una investigación de esta cuestión en el apéndice del *Algebra* de Euler, que hemos frecuentemente recomendado. Además nuestro método (partiendo de principios totalmente diferentes y no estando restringidos al caso de $m = 1$) nos da muchas formas de obtener una solución porque en el artículo 198 podemos empezar de cualquier forma reducida $(a, b, -a')$.

203.

PROBLEMA. *Si las formas* Φ *y* φ *son equivalentes, exhibir todas las transformaciones de una en la otra.*

Solución. Cuando estas formas son equivalentes de una sola manera (i.e., ya sea sólo propiamente o sólo impropiamente), por el artículo 196 se busca una transformación α, β, γ, δ de la forma φ en Φ, y es claro que todas las otras son similares a ésta. Pero cuando φ y Φ son equivalentes propia e impropiamente se buscan dos transformaciones disímiles (i.e., una propia, y la otra impropia) α, β, γ, δ; y α', β', γ', δ'; y cualquier otra transformación será similar a una de éstas. Si la forma φ es (a, b, c), su determinante es $= D$, m es el máximo común divisor de los números a, $2b$, c (como siempre fue el caso arriba), y t y u representan números indeterminados que satisfacen la ecuación $t^2 - Du^2 = m^2$, entonces en el primer caso todas las transformaciones de la forma φ en Φ estarán contenidas en la primera de las fórmulas, y en el último caso en la I o en la II.

$$\begin{array}{lll}
\text{I} \ . \ . \ . \ . & \frac{1}{m}\left(\alpha t - (\alpha b + \gamma c)u\right), & \frac{1}{m}\left(\beta t - (\beta b + \delta c)u\right) \\
& \frac{1}{m}\left(\gamma t + (\alpha a + \gamma b)u\right), & \frac{1}{m}\left(\delta t + (\beta a + \delta b)u\right) \\
\text{II} \ . \ . \ . \ . & \frac{1}{m}\left(\alpha' t - (\alpha' b + \gamma' c)u\right), & \frac{1}{m}\left(\beta' t - (\beta' b + \delta' c)u\right) \\
& \frac{1}{m}\left(\gamma' t + (\alpha' a + \gamma' b)u\right), & \frac{1}{m}\left(\delta' t + (\beta' a + \delta' b)u\right)
\end{array}$$

Ejemplo. Se desean todas las transformaciones de la forma $(129, 92, 65)$ en la forma $(42, 59, 81)$. Encontramos, en el artículo 195, que éstas son sólo impropiamente

*) Lo que Wallis, pp. 427–28, propuso para este objetivo no tiene peso. El paralogismo consiste en que, en la p. 428, línea 4, el presupone que, dada una cantidad p, pueden encontrarse enteros a y z tal que $\frac{z}{a}$ sea menor que p y que la diferencia sea menor que un número *asignado*. Esto es cierto cuando la diferencia *asignada* es una *cantidad dada* pero no cuando, como sucede en el presente caso, depende de a y z, y entonces es variable.

equivalentes y, en el artículo siguiente, que la transformación impropia de la primera en la última es -47, -56, 73, 87. Por lo tanto todas las transformaciones de la forma $(129, 92, 65)$ en $(42, 59, 81)$ serán expresadas por la fórmula

$$-(47t + 421u), \quad -(56t + 503u), \quad 73t + 653u, \quad 87t + 780u$$

donde t y u son todos los números que satisfacen la ecuación $t^2 - 79u^2 = 1$; y éstos están expresados por la fórmula

$$\pm t = \frac{1}{2}((80 + 9\sqrt{79})^e + (80 - 9\sqrt{79})^e)$$
$$\pm u = \frac{1}{2\sqrt{79}}((80 + 9\sqrt{79})^e - (80 - 9\sqrt{79})^e)$$

donde e representa a todos los enteros no negativos.

204.

Es claro que una fórmula general que represente a todas las transformaciones sería *más simple* si la transformación inicial de la cual se deduce la fórmula es más simple. Ahora, puesto que no importa desde cuál transformación empecemos, muy frecuentemente la fórmula general puede simplificarse si desde la primera fórmula encontrada deducimos una transformación menos compleja dando valores específicos a t y u, y usando esto para producir otra fórmula. Entonces, e.g., en la fórmula encontrada en el artículo precedente, al poner $t = 80$, $u = -9$, resulta una transformación que es más simple que la que encontramos. De esta forma obtenemos la transformación 29, 47, -37, -60 y la fórmula general $29t - 263u$, $47t - 424u$, $-37t + 337u$, $-60t + 543u$. Cuando, entonces, por medio de los preceptos precedentes la fórmula general es encontrada, podrá probarse si la transformación obtenida es más simple o no que aquélla de la que la fórmula fue deducida, dándole a t y u los valores específicos $\pm t'$, $\pm u'$; $\pm t''$, $\pm u''$, etc., y en este caso podrá derivarse una fórmula más simple de esa transformación. Pero qué constituye simpleza es todavía un principio arbitrario. Si fuera útil, podríamos encontrar una norma fija y asignar *límites* en las series t', u'; t'', u'', etc., más allá de las cuales las transformaciónes lleguen a ser contínuamente menos simples. Entonces no habría necesidad de buscar más y bastaría confinar nuestra búsqueda dentro de estos límites; no obstante, por brevedad suspendimos esta investigación porque muy frecuentemente mediante los métodos prescritos por nosotros surge la transformación más simple, ya sea inmediatamente o usando los valores $\pm t'$ y $\pm u'$ para t y u.

205.

PROBLEMA. *Encontrar todas las representaciones de un número dado M por una fórmula dada $ax^2 + 2bxy + cy^2$ cuyo determinante no cuadrado positivo es $= D$.*

Solución. Primero observamos que la investigación de representaciones por valores de x e y que no son primos relativos se puede reducir al caso (art. 181) de formas con determinante negativo donde se buscaron las representaciones por valores relativamente primos de las incógnitas. No hay necesidad de repetir aquí el argumento. Ahora, para representar M por valores primos relativos de x e y se requiere que D sea un residuo cuadrático de M, y si todos los valores de la expresión $\sqrt{D}$ (mod. M) son N, $-N$, N', $-N'$, N'', $-N''$, etc. (podemos escogerlos tal que ninguno sea $> \frac{1}{2}M$), entonces cualquier representación del número M por la forma dada pertenecerá a uno de estos valores. Antes de todo, se debe buscar estos valores y después investigar las representaciones que pertenecen a cada uno de ellos. No habrá ninguna representación que pertenezca al valor de N a no ser que las formas (a, b, c) y $(M, N, \frac{N^2-D}{M})$ sean propiamente equivalentes; si lo son, se busca una transformación propia α, β, γ, δ de la primera en la segunda. Entonces tendremos una representación del número M por la forma (a, b, c) perteneciente al valor N, poniendo $x = \alpha$ e $y = \gamma$, y todas las representaciones pertenecientes a este valor estarán expresadas por la fórmula

$$x = \frac{1}{m}(\alpha t - (\alpha b + \gamma c)u), \qquad y = \frac{1}{m}(\gamma t + (\alpha a + \gamma b)u)$$

donde m es el máximo común divisor de los números a, $2b$, c y t, u representan en general a todos los números que satisfacen la ecuación $t^2 - Du^2 = m^2$. Pero, manifiestamente esta fórmula general será más simple si la transformación α, β, γ, δ de la que fue deducida es más simple. Entonces será útil encontrar, según el artículo precedente, la transformación más simple de la forma (a, b, c) en $(M, N, \frac{N^2-D}{M})$ y deducir la fórmula de ésta. Exactamente de la misma manera podemos producir fórmulas generales para representaciones pertenecientes a los valores restantes $-N$, N', $-N'$ etc. (si efectivamente existe alguno).

Ejemplo. Se buscan todas las representaciones del número 585 por la fórmula $42x^2 + 62xy + 21y^2$. En relación con las representaciones por valores de x e y que no son primos relativos, es inmediatamente evidente que no puede haber otros de este tipo excepto aquéllos en los cuales el máximo común divisor de x e y sea 3, porque 585 es divisible sólo por un cuadrado, 9. Cuando encontramos, entonces, todas las representaciones del número $\frac{585}{9}$, i.e. 65 por la forma $42x'^2 + 62x'y' + 21y'^2$ con x' e y' primos relativos, podemos derivar todas las representaciones del número 585 por

la forma $42x^2 + 62xy + 21y^2$ no siendo x e y primos relativos, poniendo $x = 3x'$ e $y = 3y'$. Los valores de la expresión $\sqrt{79} \pmod{65}$ son ± 12 y ± 27. Se encuentra que la representación del número 65 perteneciente al valor -12 es $x' = 2$ e $y' = -1$. Por lo tanto todas las representaciones de 65 pertenecientes a este valor estarán expresadas por la fórmula $x' = 2t - 41u$, $y' = -t + 53u$ y *de esto* todas las representaciones de 585 por la fórmula $x = 6t - 123u$, $y = -3t + 159u$. De manera similar encontramos que la fórmula general para todas las representaciones del número 65 pertenecientes al valor 12 es $x' = 22t - 199u$, $y' = -23t + 211u$; y la fórmula para todas las representaciones del número 585 derivadas de esto será $x = 66t - 597u$, $y = -69t + 633u$. Pero, no existe una representación del número 65 perteneciente a los valores $+27$ y -27. Para encontrar representaciones del número 585 por valores x e y primos entre sí, debemos primero calcular los valores de la expresión $\sqrt{79} \pmod{585}$, los cuales son ± 77, ± 103, ± 157, ± 248. No existe ninguna representación perteneciente a los valores ± 77, ± 103 y ± 248, pero la representación $x = 3$, $y = 1$ pertenece al valor -157, y podemos deducir la fórmula general para todas las representaciones pertenecientes a este valor: $x = 3t - 114u$, $y = t + 157u$. Similarmente encontramos la representación $x = 83$, $y = -87$ perteneciente a $+157$, y la fórmula en la que todas las respresentaciones similares están contenidas es $x = 83t - 746u$, $y = -87t + 789u$. Tenemos entonces cuatro fórmulas generales en las que están contenidas todas las representaciones del número 585 por la forma $42x^2 + 62xy + 21y^2$:

$$\begin{aligned} x &= 6t - 123u \qquad & y &= -3t + 159u \\ x &= 66t - 597u \qquad & y &= -69t + 633u \\ x &= 3t - 114u \qquad & y &= t + 157u \\ x &= 83t - 746u \qquad & y &= -87t + 789u \end{aligned}$$

donde t y u representan en general todos los enteros que satisfacen la ecuación $t^2 - 79u^2 = 1$.

Por brevedad no nos detendremos en aplicaciones especiales del análisis precedente sobre formas con determinante no cuadrado positivo. Cualquiera podrá tener su propia lucha con éstas imitando el método de los artículos 176 y 182. Nos vamos a apresurar inmediatamente a considerar formas con determinante cuadrado positivo, que es el único caso que falta.

Formas de determinante cuadrado.

206.

PROBLEMA. *Dada la forma* (a, b, c) *con el determinante cuadrado* h^2*, donde* h *es la raíz positiva, encontrar una forma* (A, B, C) *que sea propiamente equivalente a ella, en la que* A *esté entre los límites* 0 *y* $2h - 1$ *inclusive,* B *sea* $= h$*,* $C = 0$*.*

Solución. I. Puesto que $h^2 = b^2 - ac$, tenemos $(h - b) : a = c : -(h + b)$. Sea $\beta : \delta$ igual a esta razón de modo que β sea primo a δ, y determínense α y γ tal que $\alpha\delta - \beta\gamma = 1$, lo cual puede hacerse. Por la sustitución α, β, γ, δ, la forma (a, b, c) será transformada en (a', b', c'), la cual será propiamente equivalente. Entonces se tendrá

$$\begin{aligned} b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \\ &= (h - b)\alpha\delta + b(\alpha\delta + \beta\gamma) - (h + b)\beta\gamma \\ &= h(\alpha\delta - \beta\gamma) = h \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2 \\ &= (h - b)\beta\delta + 2b\beta\delta - (h + b)\beta\delta = 0 \end{aligned}$$

Más aún, si a' está entre los límites 0 y $2h - 1$, la forma (a', b', c') satisfará todas las condiciones.

II. Pero si a' está fuera de los límites 0 y $2h - 1$, sea A el residuo positivo mínimo de a' relativo al módulo $2h$ que manifiestamente estará entre esos límites y sea $A - a' = 2hk$. Entonces la forma (a', b', c'), i.e. $(a', h, 0)$ será transformada por la sustitución 1, 0, k, 1 en la forma $(A, h, 0)$ que será propiamente equivalente a las formas (a', b', c') y (a, b, c) y satisfará todas las condiciones. Por otra parte es claro que la forma (a, b, c) será transformada en la forma $(A, h, 0)$ por la sustitución $\alpha + \beta k$, β, $\gamma + \delta k$, δ.

Ejemplo. Considere la forma (27,15,8) cuyo determinante es $= 9$. Aquí $h = 3$ y $4 : -9$ es la razón con los términos menores que es igual a las razones $-12 : 27 = 8 : -18$. Por lo tanto, con $\beta = 4$, $\gamma = -9$, $\alpha = -1$, $\gamma = 2$, la forma (a', b', c') se convierte en $(-1, 3, 0)$, que va a la forma $(5, 3, 0)$ por la sustitución 1, 0, 1, 1. Esta es entonces la forma buscada, y la forma dada se transforma en ella por la sustitución propia 3, 4, -7, -9.

A tales formas (A, B, C), en las que $C = 0$, $B = h$, y A está entre los límites 0 y $2h - 1$, las llamaremos *formas reducidas*, que deben distinguirse de las formas reducidas que tienen un determinante negativo o no cuadrado positivo.

207.

TEOREMA. *Dos formas reducidas* $(a, h, 0)$ *y* $(a', h, 0)$ *no idénticas no pueden ser propiamente equivalentes.*

Demostración. Si fueran propiamente equivalentes, la primera se transformaría en la segunda por una sustitución propia α, β, γ, δ y tendríamos las cuatro ecuaciones:

$$a\alpha^2 + 2h\alpha\gamma = a' \quad [1]$$

$$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h \quad [2]$$

$$a\beta^2 + 2h\beta\delta = 0 \quad [3]$$

$$\alpha\delta - \beta\gamma = 1 \quad [4]$$

Multiplicando la segunda ecuación por β, la tercera por α y restando, tenemos $-h(\alpha\delta - \beta\gamma)\beta = \beta h$ o, de [4], $-\beta h = \beta h$; de donde necesariamente β es $= 0$, por lo cual, usando [4], $\alpha\delta = 1$ y $\alpha = \pm 1$. Entonces de [1], $a \pm 2\gamma h = a'$, y esta ecuación no puede ser consistente a menos que $\gamma = 0$ (porque tanto a como a' por hipótesis están entre 0 y $2h - 1$), i.e. a menos que $a = a'$ o que las formas $(a, h, 0)$, $(a', h, 0)$ sean idénticas, lo que está en contra de la hipótesis .

Entonces los siguientes problemas, que ofrecían una mayor dificultad para los determinantes no cuadrados, pueden ser resueltos con muy poco esfuerzo.

I. *Dadas dos formas* F *y* F' *con el mismo determinante cuadrado investigar si son propiamente equivalentes o no.* Busquemos dos formas reducidas que sean propiamente equivalentes a las formas F y F' respectivamente. Si son idénticas, las formas dadas serán equivalentes; de otra manera, no lo serán.

II. *Dadas las mismas formas,* F *y* F'*, investigar si son impropiamente equivalentes o no.* Sea G la forma opuesta a una de las formas dadas, e.g. la forma F. Si G es propiamente equivalente a la forma F', F y F' serán propiamente equivalentes; de otra manera no lo serán.

208.

PROBLEMA. *Dadas dos formas propiamente equivalentes* F *y* F' *con determinante* h^2*, encontrar una transformación propia de una en la otra.*

Solución. Sea Φ una forma reducida propiamente equivalente a la forma F, que por hipótesis será también propiamente equivalente a la forma F'. Por el artículo 206 buscaremos una transformación propia α, β, γ, δ, de la forma F en Φ

y una transformación propia α', β', γ', δ' de la forma F' en Φ. Entonces Φ será transformada en F' por la transformación propia δ', $-\beta'$, $-\gamma'$, α' y entonces F en F' por la sustitución propia

$$\alpha\delta' - \beta\gamma', \quad \beta\alpha' - \alpha\beta', \quad \gamma\delta' - \delta\gamma', \quad \delta\alpha' - \gamma\beta'$$

Será útil desarrollar otra fórmula para la transformación de la forma F en F' para la cual no sea necesario conocer la forma reducida Φ. Supongamos que la forma

$$F = (a, b, c), \quad F' = (a', b', c'), \quad \Phi = (A, h, 0)$$

Puesto que $\beta : \gamma$ es la razón con números menores igual a las razones $h - b : a$ o $c : -(h + b)$, es fácil ver que $\frac{h-b}{\beta} = \frac{a}{\delta}$ será un *entero*, que llamaremos f, y que $\frac{c}{\beta} = \frac{-h-b}{\delta}$ será también un entero, que llamaremos g. Tenemos, sin embargo:

$$A = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \quad \text{y por lo tanto} \quad \beta A = a\alpha^2\beta + 2b\alpha\beta\gamma + c\beta\gamma^2$$

o (sustituyendo $a\beta$ por $\delta(h - b)$ y c por βg)

$$\beta A = \alpha^2\delta h + b(2\beta\gamma - \alpha\delta)\alpha + \beta^2\gamma^2 g$$

o sea (puesto que $b = -h - \delta g$)

$$\beta A = 2\alpha(\alpha\delta - \beta\gamma)h + (\alpha\delta - \beta\gamma)^2 g = 2\alpha h + g$$

Similarmente

$$\begin{aligned} \delta A &= a\alpha^2\delta + 2b\alpha\gamma\delta + c\gamma^2\delta \\ &= \alpha^2\delta^2 f + b(2\alpha\delta - \beta\gamma)\gamma - \beta\gamma^2 h \\ &= (\alpha\delta - \beta\gamma)^2 f + 2\gamma(\alpha\delta - \beta\gamma)h = 2\gamma h + f \end{aligned}$$

Por lo tanto

$$\alpha = \frac{\beta A - g}{2h}, \qquad \gamma = \frac{\delta A - f}{2h}$$

De exactamente la misma forma, poniendo

$$\frac{h - b'}{\beta'} = \frac{a'}{\delta'} = f', \qquad \frac{c'}{\beta'} = \frac{-h - b'}{\delta'} = g'$$

tenemos

$$\alpha' = \frac{\beta' A - g'}{2h}, \qquad \gamma' = \frac{\delta' A - f'}{2h}$$

Si los valores $\alpha, \gamma, \alpha', \gamma'$ son sustituidos en la fórmula que acabamos de dar para la transformación de la forma F en F', obtenemos

$$\frac{\beta f' - \delta' g}{2h}, \quad \frac{\beta' g - \beta g'}{2h}, \quad \frac{\delta f' - \delta' f}{2h}, \quad \frac{\beta' f - \delta g'}{2h}$$

en donde A ha desaparecido completamente.

Si se dan formas impropiamente equivalentes F y F' y se busca una transformación impropia de una en la otra, sea G la forma opuesta a la forma F y sea α, β, γ, δ la transformación propia de la forma G en F'. Entonces, manifiestamente α, β, $-\gamma$, $-\delta$ será la transformación impropia de al forma F en F'.

Finalmente, si las formas dadas son propia e impropiamente equivalentes, este método nos puede dar dos transformaciones, una propia y la otra impropia.

209.

Ahora sólo resta mostrar cómo deducimos de una transformación todas las otras transformaciones similares. Esto depende de la solución de la ecuación indeterminada $t^2 - h^2u^2 = m^2$, donde m es el máximo común divisor de los números a, $2b$, c y (a, b, c) es una de las formas equivalentes. Pero esta ecuación puede resolverse en sólo dos maneras, esto es, poniendo ya sea $t = m$, $u = 0$, o $t = -m$, $u = 0$. En efecto, supongamos que existe otra solución $t = T$, $u = U$, donde U no es $= 0$. Entonces, puesto que m^2 divide a $4h^2$, ciertamente obtendremos $\frac{4T^2}{m^2} = \frac{4h^2U^2}{m^2} + 4$ y tanto $\frac{4T^2}{m^2}$ como $\frac{4h^2U^2}{m^2}$ serán enteros cuadrados. Pero claramente el número 4 no puede ser la diferencia de dos enteros cuadrados, a no ser que el menor cuadrado sea 0, i.e., $U = 0$, en contra de la hipótesis. Por lo tanto, si la forma F se transforma en la forma F' por la sustitución α, β, γ, δ, no habrá otra transformación similar a ésta excepto $-\alpha$, $-\beta$, $-\gamma$, $-\delta$. Por lo tanto, si dos formas son sólo propiamente o sólo impropiamente equivalentes, habrá sólo *dos* transformaciones; pero si son propiamente e impropiamente equivalentes, habra *cuatro*, a saber, dos propias y dos impropias.

210.

Teorema. *Si dos formas reducidas* $(a, h, 0)$, $(a', h, 0)$ *son impropiamente equivalentes, resultará* $aa' \equiv m^2 \pmod{2mh}$, *donde* m *es el máximo común divisor*

de los números a, $2h$ o a', $2h$; y recíprocamente si a, $2h$ o a', $2h$ tienen el mismo máximo común divisor m y $aa' \equiv m^2 \pmod{2mh}$, las formas $(a, h, 0)$, $(a', h, 0)$ serán impropiamente equivalentes.

Demostración. I. Transfórmese la forma $(a, h, 0)$ en la forma $(a', h, 0)$ por la sustitución impropia α, β, γ, δ tal que tengamos cuatro ecuaciones

$$a\alpha^2 + 2h\alpha\gamma = a' \quad [1]$$

$$a\alpha\beta + h(\alpha\delta + \beta\gamma) = h \quad [2]$$

$$a\beta^2 + 2h\beta\delta = 0 \quad [3]$$

$$\alpha\delta - \beta\gamma = -1 \quad [4]$$

Si multiplicamos [4] por h y restamos de [2], lo cual escribimos como $[2] - h[4]$, se sigue que

$$(a\alpha + 2h\gamma)\beta = 2h \quad [5]$$

Similarmente de $\gamma\delta[2] - \gamma^2[3] - (a + a\beta\gamma + h\gamma\delta)[4]$, al borrar los términos que se cancelan, tenemos

$$-a\alpha\gamma = a + 2h\gamma\delta \qquad \text{o} \qquad -(a\alpha + 2h\gamma)\delta = a \quad [6]$$

y finalmente de $a[1] \ldots a\alpha(a\alpha + 2h\gamma) = aa'$ o

$$(a\alpha + 2h\gamma)^2 - aa' = 2h\gamma(a\alpha + 2h\gamma)$$

o

$$(a\alpha + 2h\gamma)^2 \equiv aa' \pmod{2h(a\alpha + 2h\gamma)} \quad [7]$$

Ahora de [5] y [6] se sigue que $a\alpha + 2h\gamma$ divide a $2h$ y a a, de donde también a m, que es el máximo común divisor de a y $2h$; sin embargo manifiestamente m también divide a $a\alpha + 2h\gamma$; por lo tanto necesariamente $a\alpha + 2h\gamma$ será $= +m$ o $= -m$. Y se sigue inmediatamente de [7] que $m^2 \equiv aa' \pmod{2mh}$ *Q. E. P.*

II. Si a y $2h$, a' y $2h$ tienen el mismo máximo común divisor m y además $aa' \equiv m^2 \pmod{2mh}$, entonces $\frac{a}{m}, \frac{2h}{m}, \frac{a'}{m}, \frac{aa'-m^2}{2mh}$ serán enteros. Es fácil confirmar que la forma $(a, h, 0)$ será transformada en la forma $(a', h, 0)$ por la sustitución $\frac{-a'}{m}$, $\frac{-2h}{m}$, $\frac{aa'-m^2}{2mh}$, $\frac{a}{m}$, y que esta transformación es impropia. Por lo tanto las dos formas serán impropiamente equivalentes. *Q. E. S.*

De esto puede juzgarse inmediatamente si alguna forma reducida dada $(a, h, 0)$ es impropiamente equivalente a sí misma. Esto es, si m es el máximo común divisor de los números a y $2h$, deberemos tener $a^2 \equiv m^2 \pmod{2mh}$.

211.

Todas las formas reducidas de un determinante dado h^2 son obtenidas si en la forma indefinida $(A, h, 0)$ se sustituye A por todos los $2h$ números de 0 hasta $2h-1$ inclusive. Claramente todas las formas del determinante h^2 pueden ser distribuidas en este número de *clases* y tendrán las mismas propiedades mencionadas arriba (art. 175, 195) para las clases de formas con determinantes negativos y positivos no cuadrados. Entonces todas las formas con determinante 25 serán distribuidas en diez clases, que podrán distinguirse por las formas reducidas contenidas en cada una de ellas. Las formas reducidas serán: $(0,5,0)$, $(1,5,0)$, $(2,5,0)$, $(5,5,0)$, $(8,5,0)$, y $(9,5,0)$, cada uno de los cuales es impropiamente equivalente a sí misma; $(3,5,0)$ que es impropiamente equivalente a $(7,5,0)$, y $(4,5,0)$ que es impropiamente equivalente a $(6,5,0)$.

212.

PROBLEMA. *Encontrar todas las representaciones de un número dado M por una forma dada $ax^2+2bxy+cy^2$ con determinante h^2.*

La solución de este problema puede buscarse a partir de los principios del artículo 168 exactamente de la misma manera que enseñamos arriba (art. 180, 181, 205) para formas con determinantes negativos y positivos no cuadrados. Sería superfluo repetirla aquí, puesto que no ofrece dificultad alguna. Por otro lado, no estará fuera de lugar deducir la solución de otro principio que es propio para el caso presente.

Como en los artículos 206 y 208:

$$h-b : a = c : -(h+b) = \beta : \delta$$
$$\frac{h-b}{\beta} = \frac{a}{\delta} = f; \quad \frac{c}{\beta} = \frac{-h-b}{\delta} = g$$

y se muestra sin dificultad que la forma dada es un producto de los factores $\delta x - \beta\gamma$ y $fx - gy$. Entonces es evidente que cualquier representación del número M por la forma dada debe proveer una resolución del número M en dos factores. Si, por lo tanto, todos los divisores del número M son d, d', d'', etc., (incluyendo también a 1 y M, y cada uno tomado *dos veces*, o sea positivamente y negativamente), es claro que todas las representaciones del número M serán obtenidas si se pone sucesivamente

que

$$\delta x - \beta y = d, \quad fx - gy = \frac{M}{d}$$
$$\delta x - \beta y = d', \quad fx - gy = \frac{M}{d'} \text{ etc.}$$

Los valores de x e y se derivarán de aquí, y aquellas representaciones que producen valores fraccionales de x e y deberán ser descontadas. Pero, manifiestamente, de las dos primeras ecuaciones resulta

$$x = \frac{\beta M - gd^2}{(\beta f - \delta g)d} \qquad \text{e} \qquad y = \frac{\delta M - fd^2}{(\beta f - \delta g)d}$$

Estos valores serán siempre *determinados* porque $\beta f - \delta g = 2h$ y entonces el denominador con certeza no será $= 0$. Por lo demás, por el mismo principio podríamos haber resuelto los otros problemas respecto a la resolubilidad de cualquier forma con un determinante cuadrado en dos factores; pero preferimos usar un método análogo a aquél presentado arriba para formas con determinante no cuadrado.

Ejemplo. Buscaremos todas las representaciones del número 12 por la forma $3x^2 + 4xy - 7y^2$. Esto es resuelto en los factores $x - y$ y $3x + 7y$. Todos los divisores del número 12 son ± 1, 2, 3, 4, 6, 12. Poniendo $x - y = 1$ y $3x + 7y = 12$ obtenemos $x = \frac{19}{10}$ e $y = \frac{9}{10}$, lo que debe ser rechazado porque son fracciones. De la misma manera obtenemos valores inútiles de los divisores -1, ± 3, ± 4, ± 6, ± 12; pero del divisor $+2$ se obtienen los valores $x = 2$, $y = 0$ y del divisor -2, $x = -2$, $y = 0$. No existen, por lo tanto, otras representaciones excepto estas dos.

Este método no se puede usar si $M = 0$. En este caso, manifiestamente, todos los valores de x e y deben satisfacer ya sea la ecuación $\delta x - \beta y = 0$ o $fx - gy = 0$. Todas las soluciones de la primera ecuación están contenidas en la fórmula $x = \beta z$, $y = \delta z$, donde z es cualquier entero (mientras β y δ sean primos relativos, como supusimos); similarmente, si ponemos m como el máximo común divisor de los números f y g, todas las soluciones de la segunda ecuación estarán representadas por la fórmula $x = \frac{gz}{m}$, $y = \frac{hz}{m}$. Entonces estas dos fórmulas generales incluyen en este caso a todas las representaciones del número M.

En la discusión precedente todo lo concerniente a la equivalencia, al descubrimiento de todas las transformaciones de formas, y a la representación de números dados por formas dadas ha sido explicado satisfactoriamente. Solo resta, por consiguiente, mostrar cómo juzgar si una de dos formas dadas, que no pueden ser equivalentes porque tienen *determinantes no iguales*, está contenida en la otra o no, y, en este caso, encontrar las transformaciones de la una en la otra.

Formas contenidas en otras a las cuales no son equivalentes.

213.

En los artículos 157 y 158 arriba mostramos que, si la forma f con determinante D implica a la forma F con determinante E y es transformada en ella por la sustitución α, β, γ, δ, entonces $E = (\alpha\delta - \beta\gamma)^2 D$; y que si $\alpha\delta - \beta\gamma = \pm 1$, la forma f no sólo implica a la forma F sino que es equivalente a ella. Por consiguiente, si la forma f implica a F pero no es equivalente a ésta, el cociente $\frac{E}{D}$ es un entero mayor que 1. Este es el problema que por lo tanto deberá resolverse: *juzgar cuándo una forma dada f con determinante D implica a una forma dada F con determinante* De^2 donde se supone que e es un número positivo mayor que 1. Para resolver esto, mostremos cómo asignar un número finito de formas contenidas en f, escogidas tal que si F está contenida en f, deba ser equivalente necesariamente a una de éstas.

I. Supongamos que todos los divisores positivos de un número e (incluyendo 1 y e) son m, m', m'' etc. y que $e = mn = m'n' = m''n''$ etc. Por brevedad, indicaremos por $(m; 0)$ la forma en la cual f es transformada por la sustitución propia m, 0, 0, n; por $(m; 1)$ la forma en la cual f es transformada por la sustitución propia m, 1, 0, n, etc.; y en general por $(m; k)$ la forma en la que f es cambiada por la sustitución propia m, k, 0, n. Similarmente, f será transformada por la transformación propia m', 0, 0, n' en $(m'; 0)$; por m', 0, 1, n' en $(m'; 1)$ etc.; por m'', 0, 0, n'' en $(m''; 0)$ etc.; etc. Todas estas formas estarán contenidas propiamente en f y el determinante de cada una será $= De^2$. Designaremos por Ω el conjunto de todas las formas $(m; 0)$, $(m; 1)$, $(m; 2)$, $\ldots (m; m-1)$, $(m'; 0)$, $(m'; 1)$, $\ldots (m'; m'-1)$, $(m''; 0)$, etc. Habrá $m + m' + m'' +$ etc. de ellas y es facil ver que todas serán diferentes la una de la otra.

Si, e.g., la forma f es $(2, 5, 7)$ y $e = 5$, Ω incluirá las siguientes formas $(1; 0)$, $(5; 0)$; $(5; 1)$, $(5; 2)$, $(5; 3)$, $(5; 4)$, y si son expandidas serán $(2, 25, 175)$, $(50, 25, 7)$, $(50, 35, 19)$, $(50, 45, 35)$, $(50, 55, 55)$, $(50, 65, 79)$.

II. Ahora, afirmo que si la forma F con determinante De^2 está propiamente contenida en la forma f, será necesariamente propiamente equivalente a una de las formas Ω. Supongamos que la forma f es transformada en F por la sustitución propia α, β, γ, δ; tendremos $\alpha\delta - \beta\gamma = e$. Sea n el máximo común divisor de los números γ, δ (que no pueden ser 0 al mismo tiempo) y sea $\frac{e}{n} = m$, lo que será, manifiestamente, un entero. Tómense g y h tal que $\gamma g + \delta h = n$, y finalmente sea k el residuo positivo mínimo del número $\alpha g + \beta h$ según el módulo m. Entonces la forma $(m; k)$, que está manifiestamente entre las formas Ω, será propiamente equivalente a la forma F y será

transformada en ella por la sustitución propia

$$\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h,\quad \frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g,\quad \frac{\gamma}{n},\quad \frac{\delta}{n}$$

Primeramente, es claro que estos cuatro números son enteros; *en segundo lugar*, es fácil confirmar que la sustitución es propia; *en tercer lugar*, es claro que la forma en la cual $(m;k)$ se transforma por esta sustitución es la misma en la que f*) se transforma por la sustitución

$$m(\frac{\gamma}{n}\cdot\frac{\alpha g+\beta h-k}{m}+h)+k\frac{\gamma}{n},\quad m(\frac{\delta}{n}\cdot\frac{\alpha g+\beta h-k}{m}-g)+\frac{k\delta}{n},\quad \gamma,\quad \delta$$

o puesto que $mn=e=\alpha\delta-\beta\gamma$ y entonces $\beta\gamma+mn=\alpha\delta$, $\alpha\delta-mn=\beta\gamma$, ésta es la sustitución

$$\frac{1}{n}(\alpha\gamma g+\alpha\delta h),\quad \frac{1}{n}(\beta\gamma g+\beta\delta h),\quad \gamma,\quad \delta$$

Pero $\gamma g+\delta h=n$, así que ésta es la sustitución α, β, γ, δ, i.e. por hipótesis ésta transforma f en F. Así $(m;k)$ y F serán propiamente equivalentes. *Q. E. D.*

De esto, por consiguiente, podemos siempre juzgar cuándo una forma dada f con determinante D implica propiamente a la forma F con determinante De^2. Si queremos encontrar cuándo f implica impropiamente a F, sólo necesitamos investigar cuándo la forma opuesta a F está contenida en f (art. 159).

214.

PROBLEMA. *Dadas dos formas, f con determinante D y F con determinante De^2, donde la primera implica propiamente a la segunda: encontrar todas las transformaciones propias de la forma f en F.*

Solución. Designando por Ω el mismo conjunto de formas como en el artículo precedente, extraiga de este conjunto todas las formas Φ, Φ', Φ'', etc. a las cuales F es propiamente equivalente. Cada una de estas formas proporcionará transformaciones propias de la forma f en F y cada una de ellas dará una transformación diferente, pero en total las proporcionarán todas (i.e., no habrá ninguna transformación propia de la forma f en F que no surja de una de las formas Φ, Φ', etc.). Puesto que el método es el mismo para todas las formas Φ, Φ', etc., hablamos de sólo una de ellas.

*) En efecto se transforma en $(m;K)$ por la sustitución m, K, 0, n. Vea artículo 159.

Supongamos que Φ es $(M;K)$ y $e = MN$ de manera que f se transforme en Φ por la sustitución propia M, K, 0, N. Además desígnense todas las transformaciones propias de la forma Φ en F en general por $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$. Entonces claramente f se transformará en Φ por la substitución propia $M\mathfrak{a} + K\mathfrak{c}$, $M\mathfrak{b} + K\mathfrak{d}$, $N\mathfrak{c}$, $N\mathfrak{d}$ y de esta manera cualquier transformación propia de la forma Φ en F dará una transformación propia de la forma f en F. Las otras formas Φ', Φ'', etc. se tratan del mismo modo, y cada transformación propia de una de éstas en F dará lugar a una transformación propia de la forma f en F.

Para mostrar que esta solución es completa en todo aspecto, se mostrará

I. *Que todas las transformaciones propias posibles de la forma f en F se obtienen de este modo.* Sea α, β, γ, δ cualquier transformación propia de la forma f en F y como en el artículo anterior, parte II, sea n el máximo común divisor de los números γ y δ; y sean los números m, g, h, k determinados tal como lo fueron allí. Entonces la forma $(m;k)$ estará entre las formas Φ, Φ', etc. y

$$\frac{\gamma}{n} \cdot \frac{\alpha g + \beta h - k}{m} + h, \quad \frac{\delta}{n} \cdot \frac{\alpha g + \beta h - k}{m} - g, \quad \frac{\gamma}{n}, \quad \frac{\delta}{n}$$

será una de las transformaciones propias de esta forma en F; a partir de ésta, por la regla que acabamos de dar, se obtiene la transformación α, β, γ, δ; todo esto fue demostrado en el artículo precedente.

II. *Que todas las transformaciones obtenidas de esta manera son diferentes entre sí; esto es, ninguna de ellas se obtiene dos veces.* Es fácil ver que transformaciones diferentes de la misma forma Φ o Φ', etc. en F no pueden producir la misma transformación de f en F; se muestra de la siguiente manera que formas diferentes, por ejemplo Φ y Φ', no pueden producir la misma transformación. Supongamos que la transformación propia α, β, γ, δ de la forma f en F se obtiene *tanto de la transformación propia* $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, $\mathfrak{d}$ *de la forma* Φ *en* F *como* de la transformación propia $\mathfrak{a}'$, $\mathfrak{b}'$, $\mathfrak{c}'$, $\mathfrak{d}'$ de la forma Φ' en F. Sean $\Phi = (M;K)$, $\Phi' = (M';K')$ y $e = MN = M'N'$. Habrá estas ecuaciones:

$$\alpha = M\mathfrak{a} + K\mathfrak{c} = M'\mathfrak{a}' + K'\mathfrak{c}' \quad [1]$$

$$\beta = M\mathfrak{b} + K\mathfrak{d} = M'\mathfrak{b}' + K'\mathfrak{d}' \quad [2]$$

$$\gamma = N\mathfrak{c} = N'\mathfrak{c}' \quad [3]$$

$$\delta = N\mathfrak{d} = N'\mathfrak{d}' \quad [4]$$

$$\mathfrak{a}\mathfrak{d} - \mathfrak{b}\mathfrak{c} = \mathfrak{a}'\mathfrak{d}' - \mathfrak{b}'\mathfrak{c}' = 1 \quad [5]$$

De $\mathfrak{a}[4]-\mathfrak{b}[3]$ y usando ecuación [5] se sigue que $N = N'(\mathfrak{a}\mathfrak{d}'-\mathfrak{b}\mathfrak{c}')$, y de este modo N' divide a N; de manera análoga, de $\mathfrak{a}'[4]-\mathfrak{b}'[3]$ resulta $N' = N(\mathfrak{a}'\mathfrak{d}-\mathfrak{b}'\mathfrak{c})$ y N divide a N', de donde, dado que ambos N y N' se suponen positivos, tenemos necesariamente $N = N'$ y $M = M'$ y así de [3] y [4], $\mathfrak{c} = \mathfrak{c}'$ y $\mathfrak{d} = \mathfrak{d}'$. Además, de $\mathfrak{a}[2] - \mathfrak{b}[1]$,

$$K = M'(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'(\mathfrak{a}\mathfrak{d}' - \mathfrak{b}\mathfrak{c}') = M(\mathfrak{a}\mathfrak{b}' - \mathfrak{b}\mathfrak{a}') + K'$$

de aquí $K \equiv K'$ (mod. M), lo que no puede ser cierto a menos que $K = K'$, porque ambos K y K' se encuentran entre los límites 0 y $M - 1$. Por lo tanto las formas Φ y Φ' no son diferentes, contrariamente a la hipótesis.

Es claro que si D es negativo o un cuadrado positivo, este método nos dará todas las transformaciones propias de la forma f en F; y si D es positivo no cuadrado, pueden darse ciertas fórmulas generales que contendrán todas las transformaciones propias (su número es infinito).

Finalmente, si la forma F está impropiamente contenida en la forma f, todas las transformaciones impropias de la primera en la última pueden encontrarse fácilmente por el método dado. A saber, si α, β, γ, δ designan en general todas las transformaciones propias de la forma f en la forma opuesta a la forma F, todas las transformaciones impropias de la forma f en F serán representadas por α, $-\beta$, γ, $-\delta$.

Ejemplo. Se desean todas las transformaciones de la forma $(2, 5, 7)$ en $(275, 0, -1)$, la cual está contenida en ella tanto propia como impropiamente. En el artículo precedente dimos el conjunto de las formas Ω para este caso. Después de unos cálculos, se encuentra que tanto $(5; 1)$ como $(5; 4)$ son propiamente equivalentes a la forma $(275, 0, -1)$. Todas las transformaciónes propias de la forma $(5; 1)$, i.e., $(50, 35, 19)$ en $(275, 0, -1)$, se pueden hallar por nuestra teoría arriba dentro de la fórmula general

$$16t - 275u, \quad -t + 16u, \quad -15t + 275u, \quad t - 15u$$

donde t y u son representaciones indeterminadas de todos los enteros que satisfacen la ecuación $t^2 - 275u^2 = 1$; por lo tanto todas las transformaciones propias de la forma $(2, 5, 7)$ en $(275, 0, -1)$ estarán contenidas en la fórmula general

$$65t - 1100u, \quad -4t + 65u, \quad -15t + 275u, \quad t - 15u.$$

De manera análoga, todas las transformaciones propias de la forma $(5;4)$, i.e., $(50,65,79)$ en $(275,0,-1)$, están contenidas en la fórmula general

$$14t+275u, \quad t+14u, \quad -15t-275u, \quad -t-15u$$

y así todas las transformaciones propias de la forma $(2,5,7)$ en $(275,0,-1)$ estarán contenidas en

$$10t+275u, \quad t+10u, \quad -15t-275u, \quad -t-15u$$

Por lo tanto, estas dos fórmulas incluyen todas las transformaciones propias que buscamos*). De la misma manera se encuentra que todas las transformaciones impropias de la forma $(2,5,7)$ en $(275,0,-1)$ están contenidas en las dos fórmulas siguientes:

$$\text{(I)} \quad \ldots \quad 65t-1100u, \quad 4t-65u, \quad -15t+275u, \quad -t+15u$$

y

$$\text{(II)} \quad \ldots \quad 10t+275u, \quad -t-10u, \quad -15t-275u, \quad t+15u$$

Formas con determinante 0.

215.

Hasta ahora hemos excluido de todas las investigaciones las formas con determinante 0; ahora agreguemos algo acerca de estas formas para que nuestra teoría sea completa en todos los sentidos. Dado que se mostró en general que, si una forma con determinante D implica a una forma con determinante D', D' es un múltiplo de D, es inmediatamente claro que una forma cuyo determinante es igual a cero no puede implicar a otra forma a menos que su determinante también sea igual a cero. Así solamente dos problemas quedan por resolver, a saber: (1) *dadas dos formas f y F, donde F tiene determinante 0, juzgar si f implica a F o no, y,*

*) Más concisamente, todas las transformaciones propias se incluyen en la fórmula

$$10t+55u, \quad t+2u, \quad -15t-55u, \quad -t-3u$$

donde t y u son todos los enteros que satisfacen la ecuación $t^2-11u^2=1$.

en ese caso, exhibir todas las transformaciones involucradas; (2)*, encontrar todas las representaciones de un número dado por una forma dada con determinante 0.* El primer problema requiere de un método cuando el determinante de la forma f es también 0, otro cuando no es 0. Ahora explicamos todo esto.

I. Antes de todo observamos que cualquier forma $ax^2 + 2bxy + cy^2$ cuyo determinante es $b^2 - ac = 0$ puede ser expresada como $m(gx + hy)^2$ donde g y h son primos relativos y m un entero. Pues, sea m el máximo común divisor de a y c con el mismo signo que ellos (es fácil ver que ellos no pueden poseer signos opuestos), entonces $\frac{a}{m}$ y $\frac{c}{m}$ serán enteros primos relativos no negativos, y su producto será igual a $\frac{b^2}{m^2}$, i.e., un cuadrado, y así cada uno de ellos será también un cuadrado (art. 21). Sean $\frac{a}{m} = g^2$ y $\frac{c}{m} = h^2$ con g y h también primos relativos, y tenemos $g^2h^2 = \frac{b^2}{m^2}$ y $gh = \pm\frac{b}{m}$. Así es claro que

$$m(gx \pm hy)^2 \qquad \text{será} \qquad = ax^2 + 2bxy + cy^2$$

Sean ahora f y F dos formas dadas, cada una con determinante 0 y con

$$f = m(gx + hy)^2, \qquad F = M(GX + HY)^2$$

donde g y h, G y H son primos relativos. Afirmo ahora que si la forma f implica a la forma F, m es igual a M o al menos divide a M, y el cociente es un cuadrado; y, recíprocamente, si $\frac{M}{m}$ es un entero cuadrado, F está contenida en f. Pues si se asume que f se transforma en F, por la substitución

$$x = \alpha X + \beta Y, \qquad y = \gamma X + \delta Y$$

resultará

$$\frac{M}{m}(GX + HY)^2 = ((\alpha g + \gamma h)X + (\beta g + \delta h)Y)^2$$

y se sigue fácilmente que $\frac{M}{m}$ es un cuadrado. Igualándole a e^2, tenemos

$$e(GX + HY) = \pm\left((\alpha g + \gamma h)X + (\beta g + \delta h)Y\right), \quad \text{i.e.}$$
$$\pm eG = \alpha g + \gamma h, \quad \pm eH = \beta g + \delta h$$

Por lo tanto si $\mathfrak{G}$ y $\mathfrak{H}$ se determinan de modo que $\mathfrak{G}G + \mathfrak{H}H = 1$ obtenemos

$$\pm e = \mathfrak{G}(\alpha g + \gamma h) + \mathfrak{H}(\beta g + \delta h), \qquad \text{y por ende un } \textit{entero.} \quad \textit{Q. E. P.}$$

Si, recíprocamente, se supone que $\frac{M}{m}$ es un entero cuadrado igual a e^2, la forma f implicará a la forma F. Esto es, los enteros α, β, γ, δ pueden determinarse de modo que

$$\alpha g + \gamma h = \pm eG, \qquad \beta g + \delta h = \pm eH$$

Pues si se encuentran enteros $\mathfrak{g}$ y $\mathfrak{h}$ de modo que $\mathfrak{g}g + \mathfrak{h}h = 1$, podemos satisfacer estas ecuaciones poniendo:

$$\alpha = \pm eG\mathfrak{g} + hz, \qquad \gamma = \pm eG\mathfrak{h} - gz$$
$$\beta = \pm eH\mathfrak{g} + hz', \qquad \delta = \pm eH\mathfrak{h} - gz'$$

donde z y z' pueden tomar valores enteros cualesquiera. Así F estará contenida en f. *Q. E. S.* Al mismo tiempo no es difícil ver que estas fórmulas dan todos los valores que α, β, γ, δ pueden asumir, i.e., todas las transformaciones de la forma f en F, a condición que z y z' asuman todos los valores enteros.

II. Propuestas las dos formas $f = ax^2 + 2bxy + cy^2$ cuyo determinante no es igual a 0, y $F = M(GX + HY)^2$ cuyo determinante es igual a 0 (aquí como antes G y H son primos entre si), afirmo *primero* que si f implica a F, el número M puede representarse por la forma f; *segundo*, si M puede representarse por f, F estará contenida en f; *tercero*, si en este caso todas las representaciones del número M por la forma f pueden ser exhibidas en términos generales por $x = \xi$ e $y = \nu$, todas las transformaciones de la forma f en F pueden exhibirse por $G\xi$, $H\xi$, $G\nu$, $H\nu$. Mostramos todo esto de la siguiente manera.

1^o Suponga que f se transforma en F por la substitución α, β, γ, δ y tómense números $\mathfrak{G}$, $\mathfrak{H}$ de modo que $\mathfrak{G}G + \mathfrak{H}H = 1$. Entonces si hacemos $x = \alpha\mathfrak{G} + \beta\mathfrak{H}$, $y = \gamma\mathfrak{G} + \delta\mathfrak{H}$, el valor de la forma f se hará M y así M es representable por la forma f.

2^o Si se supone que $a\xi^2 + 2b\xi\nu + c\nu^2 = M$, por la substitución $G\xi$, $H\xi$, $G\nu$, $H\nu$ la forma f se transformará en F.

3^o En este caso la substitución $G\xi$, $H\xi$, $G\nu$, $H\nu$ presentará todas las transformaciones de la forma f en F si se supone que ξ y ν recorren todos los valores de x e y que hacen $f = M$; se muestra esto del siguiente modo. Sea α, β, γ, δ cualquier transformación de la forma f en F y sea como antes $\mathfrak{G}G + \mathfrak{H}H = 1$. Entonces entre los valores de x e y estarán también éstos:

$$x = \alpha\mathfrak{G} + \beta\mathfrak{H}, \qquad y = \gamma\mathfrak{G} + \delta\mathfrak{H}$$

de los cuales se obtiene la substitución

$$G(\alpha\mathfrak{G}+\beta\mathfrak{H}), \qquad H(\alpha\mathfrak{G}+\beta\mathfrak{H}), \qquad G(\gamma\mathfrak{G}+\delta\mathfrak{H}), \qquad H(\gamma\mathfrak{G}+\delta\mathfrak{H})$$

o

$$\alpha+\mathfrak{H}(\beta G-\alpha H), \quad \beta+\mathfrak{G}(\alpha H-\beta G), \quad \gamma+\mathfrak{H}(\delta G-\gamma H), \qquad \delta+\mathfrak{H}(\gamma H-\gamma G).$$

Pero ya que

$$a(\alpha X+\beta Y)^2+2b(\alpha X+\beta Y)(\gamma X+\delta Y)+c(\gamma X+\delta Y)^2=M(GX+HY)^2$$

resultará

$$a(\alpha\delta-\beta\gamma)^2=M(\delta G-\gamma H)^2$$
$$c(\beta\gamma-\alpha\delta)^2=M(\beta G-\alpha H)^2$$

y así (ya que el determinante de la forma f multiplicado por $(\alpha\delta-\beta\gamma)^2$ es igual al determinante de la forma F, i.e., igual a 0, y así también $\alpha\delta-\beta\gamma=0$),

$$\delta G-\gamma H=0, \qquad \beta G-\alpha H=0$$

Por consiguiente la substitución en cuestión se reduce a α, β, γ, δ, y la fórmula que estamos considerando produce *todas* las transformaciones de la forma f en F.

III. Queda por mostrar cómo podemos exhibir todas las representaciones de un número dado por una forma dada con determinante 0. Sea esta forma $m(gx+hy)^2$, y es claro inmediatamente que el número debe ser divisible por m y que su cociente es un cuadrado. Si por lo tanto representamos al número dado por me^2, los valores de x e y que hacen $m(gx+hy)^2=me^2$ serán aquellos valores para los cuales $gx+hy$ sea igual a $+e$ o a $-e$. Así se tendrán todas las representaciones si se encuentran todas las soluciones enteras de las ecuaciones lineales $gx+hy=e$ y $gx+hy=-e$. Es claro que éstas son resolubles (si verdaderamente g y h son primos relativos como se supone). Esto es, si $\mathfrak{g}$ y $\mathfrak{h}$ son determinados de modo que $\mathfrak{g}g+\mathfrak{h}h=1$, la primera ecuación se satisfará poniendo $x=\mathfrak{g}e+hz$, $y=\mathfrak{h}e-gz$; la segunda tomando $x=-\mathfrak{g}e+hz$, $y=-\mathfrak{h}e-gz$ con z cualquier entero. Al mismo tiempo estas fórmulas darán *todos* los valores enteros de x e y si z representa en general a cualquier entero.

Solución general de toda ecuación indeterminada de segundo grado con dos incógnitas por numeros enteros.

Habiendo concluido exitosamente estas investigaciones, proseguimos.

216.

PROBLEMA. *Encontrar todas las soluciones enteras para la ecuación general**) indeterminada de segundo grado con dos incógnitas

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$$

(donde a, b, c, etc. son cualesquiera enteros dados).

Solución. En lugar de las incógnitas x e y introducimos otras

$$p = (b^2 - ac)x + be - cd \qquad \text{y} \qquad q = (b^2 - ac)y + bd - ae$$

que siempre serán enteros cuando x e y son enteros. Ahora resulta la ecuación

$$ap^2 + 2bpq + cq^2 + f(b^2 - ac)^2 + (b^2 - ac)(ae^2 - 2bde + cd^2) = 0$$

o si por brevedad escribimos

$$f(b^2 - ac)^2 + (b^2 - ac)(ae^2 - 2bde + cd^2) = -M$$

se da

$$ap^2 + 2bpq + cq^2 = M$$

Mostramos en la sección precedente cómo encontrar todas las soluciones de esta ecuación, i.e., todas las representaciones del número M por la forma (a, b, c). Ahora si para cada valor de p y q determinamos los valores correspondientes de x e y con la ayuda de las ecuaciones

$$x = \frac{p + cd - be}{b^2 - ac}, \qquad y = \frac{q + ae - bd}{b^2 - ac}$$

es fácil ver que todos estos valores satisfacen la ecuación dada y que no existen valores enteros de x e y que no se incluyen. Si por lo tanto eliminamos las fracciones entre todos los valores de x e y así obtenidos, todas las soluciones que deseamos permanecerán.

Con respecto a estas soluciones se observa lo siguiente.

---

*) Si se propusiera una ecuación en la cual el segundo, cuarto o quinto coeficiente no fuera par, su multiplicación por 2 produciría la forma que suponemos aquí.

1^o Si M no puede representarse por la forma $(a,\ b,\ c)$ o si no se obtienen valores *enteros* de x e y de ninguna representación, la ecuación no puede resolverse por enteros del todo.

2^o Cuando el determinante de la forma (a, b, c), i.e. el número $b^2 - ac$, es negativo o un cuadrado positivo y al mismo tiempo M no es igual a 0, el número de representaciones del número M será finito y así también el número de soluciones de la ecuación dada (si es que existe alguna) será finito.

3^o Cuando $b^2 - ac$ es positivo no cuadrado, o cuadrado con M igual a 0, el número M podrá representarse *en infinitamente distintas maneras* por la forma (a, b, c) si es que puede representarse de alguna manera. Pero dado que es imposible encontrar todas estas representaciones *individualmente* y examinar si ellas dan valores enteros o fraccionarios de x e y, es necesario establecer una regla bajo la cual podamos tener *certeza* de cuando ninguna representación en absoluto produce valores enteros de x e y (puesto que no importa cuántas representaciones se intenten, sin una regla tal nunca estaremos seguros). Y cuando algunas representaciones dan valores enteros de x e y y otras dan fracciones, debe determinarse cómo distinguir en general una de la otra.

4^o Cuando $b^2 - ac = 0$, los valores de x e y no pueden determinarse del todo por las fórmulas precedentes; por lo tanto para este caso necesitaremos recurrir a un *método especial*.

217.

Para el caso donde $b^2 - ac$ es un número positivo no cuadrado, mostramos arriba que todas las representaciones del número M por la forma $ap^2 + 2bpq + cq^2$ (si es que existe alguna) pueden exhibirse por una o por varias fórmulas como la siguiente:

$$p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

donde $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ son enteros dados, m es el máximo común divisor de los números a, $2b$ y c, finalmente t y u son en general todos los enteros que satisfacen la ecuación $t^2 - (b^2 - ac)u^2 = m^2$. Como todos los valores de t y u pueden tomarse tanto positiva como negativamente, para cada una de estas formas podemos substituir otras *cuatro*:

$$p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$
$$p = \frac{1}{m}(\mathfrak{A}t - \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t - \mathfrak{D}u)$$
$$p = \frac{1}{m}(-\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(-\mathfrak{C}t + \mathfrak{D}u)$$
$$p = -\frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = -\frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u)$$

de modo que el número de fórmulas es ahora cuatro veces lo que era antes, y t y u ya no son todos los números que satisfacen la ecuación $t^2 - (b^2 - ac)a^2 = m^2$ sino solamente los valores positivos. Por lo tanto cada una de estas formas será considerada separadamente, y debe investigarse cuáles valores de t y u dan valores enteros de x e y.

De la fórmula

$$p = \frac{1}{m}(\mathfrak{A}t + \mathfrak{B}u), \qquad q = \frac{1}{m}(\mathfrak{C}t + \mathfrak{D}u) \qquad [1]$$

los valores de x e y serán éstos:

$$x = \frac{\mathfrak{A}t + \mathfrak{B}u + mcd - mbe}{m(b^2 - ac)}, \qquad y = \frac{\mathfrak{C}t + \mathfrak{D}u + mae - mbd}{m(b^2 - ac)}$$

Demostramos antes que todos los valores (positivos) de t forman una serie recurrente t^0, t', t'', etc. y similarmente, que los valores correspondientes de u también forman una serie recurrente u^0, u', u'', etc.; y que además puede asignarse un número ρ tal que según cualquier módulo dado tengamos

$$t^\rho \equiv t^0,\ t^{\rho+1} \equiv t',\ t^{\rho+2} \equiv t'' \text{ etc.}, \quad u^\rho \equiv u^0,\ u^{\rho+1} \equiv u',\ \text{etc.}$$

Tomaremos para este módulo el número $m(b^2 - ac)$ y por brevedad designaremos por x^0 e y^0 los valores de x e y que se obtienen haciendo $t = t^0$, $u = u^0$; de la misma manera x' e y' designarán los valores que se obtienen haciendo $t = t'$ y $u = u'$, etc. Entonces no es difícil notar que si x^h e y^h son enteros y ρ apropiadamente escogido, $x^{h+\rho}$ e $y^{h+\rho}$, $x^{h+2\rho}$ e $y^{h+2\rho}$ y, en general, $x^{h+k\rho}$ e $y^{h+k\rho}$ también serán enteros; y recíprocamente, si x^h o y^h es una fracción, $x^{h+k\rho}$ o $y^{h+k\rho}$ será también una fracción. Se concluye que si uno revisa los valores de x e y correspondientes a los índices 0, 1, 2, $\ldots \rho - 1$ y encuentra que no hay uno de ellos para el cual *tanto x como y* sea

entero, entonces no existen en absoluto índices, para los cuales ambos x e y posean valores enteros, y así de la fórmula [1] no se pueden deducir valores enteros de x e y. Pero si existen algunos índices, digamos μ, μ', μ'', etc., para los cuales x e y poseen valores enteros, entonces todos los valores de x e y que pueden obtenerse a partir de la fórmula [1] serán aquéllos cuyos índices estén contenidos en una de las fórmulas $\mu + k\rho$, $\mu' + k\rho$, $\mu'' + k\rho$, etc., donde k es cualquier entero positivo incluyendo al cero.

Las otras fórmulas que contienen los valores de p y q pueden tratarse exactamente de la misma manera. Si se diera el caso que de ninguna de éstas se obtienen valores enteros de x e y, entonces la ecuación propuesta no puede ser resuelta por enteros. Pero cuando ésta puede ser resuelta, todas las soluciones enteras se pueden mostrar por medio de las reglas precedentes.

218.

Cuando $b^2 - ac$ es un cuadrado y M es igual a cero, todos los valores de p y q están incluidos en dos fórmulas de la forma $p = \mathfrak{A}z$, $q = \mathfrak{B}z$ o $p = \mathfrak{A}'z$, $q = \mathfrak{B}'z$, donde z indica de modo indefinido a cualquier entero, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{A}'$, $\mathfrak{B}'$ son enteros dados, y el primero y el segundo no han de poseer un divisor común, ni tampoco el tercero y el cuarto (art. 212). Todos los valores enteros de x e y que surgen de la primera fórmula estarán contenidos en la fórmula [1]:

$$x = \frac{\mathfrak{A}z + cd - be}{b^2 - ac}, \qquad y = \frac{\mathfrak{B}z + ae - bd}{b^2 - ac}$$

y todos los otros que surjan de la segunda fórmula estarán contenidos en [2]:

$$x = \frac{\mathfrak{A}'z + cd - be}{b^2 - ac}, \qquad y = \frac{\mathfrak{B}'z + ae - bd}{b^2 - ac}$$

Pero dado que cada fórmula puede producir valores fraccionarios (a menos que $b^2 - ac = 1$), es necesario separar de los otros, en cada fórmula, aquellos valores de z que hacen a ambos x e y enteros. Sin embargo, es suficiente considerar la primera fórmula solamente, dado que exactamente el mismo método puede usarse para la otra.

Como $\mathfrak{A}$ y $\mathfrak{B}$ son primos relativos, se pueden determinar dos números $\mathfrak{a}$ y $\mathfrak{b}$ tales que $\mathfrak{a}\mathfrak{A} + \mathfrak{b}\mathfrak{B} = 1$. De esto se obtiene

$$(\mathfrak{a}x + \mathfrak{b}y)(b^2 - ac) = z + \mathfrak{a}(cd - be) + \mathfrak{b}(ae - bd)$$

De esto es inmediatamente claro que todos los valores de z que producen valores enteros de x e y deben ser congruentes al número $\mathfrak{a}(be-cd)+\mathfrak{b}(bd-ae)$ según el módulo b^2-ac, o deben estar contenidos en la fórmula $(b^2-ac)z'+\mathfrak{a}(be-cd)+\mathfrak{b}(bd-ae)$ donde z' designa cualquier entero. Entonces en lugar de la fórmula [1] obtenemos fácilmente la siguiente:

$$x = \mathfrak{A}z' + \mathfrak{b}\frac{\mathfrak{A}(bd-ae)-\mathfrak{B}(be-cd)}{b^2-ac}$$
$$y = \mathfrak{B}z' - \mathfrak{a}\frac{\mathfrak{A}(bd-ae)-\mathfrak{B}(be-cd)}{b^2-ac}$$

Queda de manifiesto que ésta da valores enteros para x e y ambos para todos los valores de z' o para ninguno. Lo primero será cierto cuando $\mathfrak{A}(bd-ae)$ y $\mathfrak{B}(be-cd)$ sean congruentes según el módulo b^2-ac, el último cuando ellos no sean congruentes. Podemos tratar la fórmula [2] exactamente de la misma manera y separar las soluciones enteras (si existe alguna) del resto.

219.

Cuando $b^2-ac=0$, la forma $ax^2+2bxy+cy^2$ puede expresarse como $m(\alpha x+\beta y)^2$ donde m, α, β son enteros (art. 215). Si se pone $\alpha x+\beta y=z$, la ecuación se convertirá en:

$$mz^2+2dx+2ey+f=0$$

De esto y del hecho que $z=\alpha x+\beta y$ deducimos que

$$x=\frac{\beta mz^2+2ez+\beta f}{2\alpha e-2\beta d}, \qquad y=\frac{\alpha mz^2+2dz+\alpha f}{2\beta d-2\alpha e}$$

Ahora es claro que si no fuera $\alpha e=\beta d$ (consideraremos este caso por separado de inmediato), los valores de x e y obtenidos a medida que z toma cualquier valor en estas fórmulas, satisfarán la ecuación dada; por lo tanto, sólo queda por demostrar cómo determinar los valores de z que darán valores enteros de x e y.

Dado que $\alpha x+\beta y=z$, puede escogerse sólo valores *enteros* para z. Además es claro que si cualquier valor de z da valores enteros tanto para x como para y, todos los valores congruentes con z según el módulo $2\alpha e-2\beta d$ producirán de la

misma manera valores enteros. Por esto si se substituyen en z todos los enteros de 0 a $2\alpha e - 2\beta d - 1$ (cuando $\alpha e - \beta d$ es positivo) o inclusive a $2\beta d - 2\alpha e - 1$ (cuando $\alpha e - \beta d$ es negativo), y si para ninguno de estos valores se hacen x e y enteros, entonces ningún valor de z producirá valores enteros para x e y, y la ecuación dada no podrá resolverse por enteros. Pero si x e y poseen valores enteros para alguno de esos valores de z, digamos ζ, ζ', ζ'', etc., (ellos también pueden hallarse resolviendo la congruencia de segundo grado de acuerdo con los principios de la sección IV), se encuentran *todas* las soluciones poniendo $z = (2\alpha e - 2\beta d)\nu + \zeta$, $z = (2\alpha e - 2\beta d)\nu + \zeta'$, etc., con ν tomando todos los valores enteros.

220.

Es conveniente indagar un método especial para el caso que hemos excluído, donde $\alpha e = \beta d$. Supongamos que α y β son primos entre sí, lo cual es posible por el artículo 215.I; así $\frac{d}{\alpha} = \frac{e}{\beta}$ será un entero (art. 19), que llamamos h. Entonces, la ecuación dada tomará esta forma:

$$(m\alpha x + m\beta y + h)^2 - h^2 + mf = 0$$

y claramente ésta no puede resolverse racionalmente, a menos que $h^2 - mf$ sea un cuadrado. Sea $h^2 - mf = k^2$, y la ecuación dada será equivalente a las siguientes dos:

$$m\alpha x + m\beta y + h + k = 0, \qquad m\alpha x + m\beta y + h - k = 0$$

i.e., cualquier solución de la ecuación dada satisfará una u otra de estas ecuaciones y viceversa. Obviamente la primera ecuación no puede resolverse por enteros a menos que $h + k$ sea divisible por m, y, similarmente, la segunda ecuación no admitirá solución por enteros a no ser que $h - k$ sea divisible por m. Estas condiciones son suficientes para resolver todas las ecuaciones (porque nosotros asumimos que α y β son primos entre sí) y puede encontrarse todas las soluciones usando reglas bien conocidas.

221.

Ilustramos con un ejemplo el caso del artículo 217 (pues éste es el más difícil). Sea $x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$ la ecuación dada. Por la introducción de otros indeterminados $p = 15x - 9$ y $q = 15y + 6$, se deriva la ecuación $p^2 + 8py + q^2 = -540$.

Todas las soluciones por enteros de esta ecuación se encuentran por consiguiente contenidas en las siguientes cuatro fórmulas:

$$\begin{aligned} p &= 6t, & q &= -24t - 90u \\ p &= 6t, & q &= -24t + 90u \\ p &= -6t, & q &= 24t - 90u \\ p &= -6t, & q &= 24t + 90u \end{aligned}$$

donde t y u denotan todos los enteros positivos que satisfacen la ecuación $t^2 - 15u^2 = 1$, y ellos se expresan por la fórmula:

$$\begin{aligned} t &= \frac{1}{2}\left((4+\sqrt{15})^n + (4-\sqrt{15})^n\right) \\ u &= \frac{1}{2\sqrt{15}}\left((4+\sqrt{15})^n - (4-\sqrt{15})^n\right) \end{aligned}$$

donde n designa a todos los enteros positivos (incluido el cero). Por esto todos los valores de x e y estarán contenidos en estas fórmulas

$$\begin{aligned} x &= \frac{1}{5}(2t+3), & y &= -\frac{1}{5}(8t+30u+2) \\ x &= \frac{1}{5}(2t+3), & y &= -\frac{1}{5}(8t-30u+2) \\ x &= \frac{1}{5}(-2t+3), & y &= \frac{1}{5}(8t-30u-2) \\ x &= \frac{1}{5}(-2t+3), & y &= \frac{1}{5}(8t+30u-2) \end{aligned}$$

Si aplicamos correctamente lo que hemos dicho arriba, descubrimos que para producir enteros debemos usar en la primera y segunda fórmulas valores de t y u que vienen de tomar n *par*; en la tercera y cuarta de tomar n *impar*. Las soluciones más simples son: $x = 1, -1, -1$ e $y = -2, 0, 12$ respectivamente.

Por otra parte, observamos que la solución del problema en los artículos precedentes puede a menudo acortarse por varios artificios especialmente ideados para excluir soluciones inútiles, i.e., fracciones; pero debemos omitir esta discusión a fin de no prolongar nuestra discusión más allá de los límites.

Anotaciones Históricas.

222.

Dado que mucho de lo que hemos explicado también ha sido tratado por otros geómetras, no podemos pasar sobre sus trabajos en silencio. El ilustre Lagrange emprendió investigaciones generales concernientes a la *equivalencia de las formas* en *Nouv. Mém. de l'Ac. de Berlin*, 1773, *p.* 263 y 1775, *p.* 323 y siguientes, donde él mostró, que para un determinante dado, puede encontrarse un número finito de formas tales que cada forma de ese determinante sea equivalente a una de éstas, y así que todas las formas de un determinante dado pueden distribuirse en clases. Más tarde el distinguido Legendre descubrió, en gran parte por inducción, muchas propiedades elegantes de esta clasificación, cuyas demostraciones presentaremos más abajo. Hasta aquí nadie ha usado la distinción entre equivalencia propia e impropia, pero este es un instrumento muy efectivo para investigaciones más sutiles.

Lagrange fue el primero en resolver completamente el famoso problema del artículo 216 y siguientes, *Hist. de l'Ac. de Berlin*, 1767, *p.* 165 y 1768 *p.* 181 y siguientes. También existe una solución (pero menos completa) en el suplemento al *Algebra* de Euler, el cual hemos nombrado regularmente. El mismo Euler atacó este problema en *Comm. Petr., T.* VI, *p.* 175, *Comm. Nov., T.* IX, *p.* 3; *Ibid., T.* 18, *p.* 185 y siguientes, pero él siempre restringió su investigación a derivar otras soluciones de una que él asumía ya conocida; además, sus métodos pueden dar *todas* las soluciones en solamente unos cuantos casos (véase Lagrange *Hist. de l'Ac. de Berlin*, 1767, *p.* 237). Ya que el último de estos tres comentarios es de fecha más reciente que la solución de Lagrange, que trata el problema con toda generalidad y no deja nada que desear en este aspecto, parece que Euler no sabía entonces de esa solución (el Vol. 18 de los *Commentarii* corresponde al año 1773 y fue publicado en 1774). Por lo demás, nuestra solución (al igual que todas las cosas discutidas en esta sección) es construida sobre principios totalmente diferentes.

Lo que Diofanto, Fermat, etc., entre otros, han tratado en relación con este tema pertenece solamente a casos especiales; por esto, ya que arriba hemos mencionado lo más digno de notar, no lo discutiremos separadamente.

Lo que ha sido dicho hasta aquí acerca de las formas de segundo grado debe ser considerado solamente como los primeros principios de esta teoría. El campo dejado para investigación posterior parece muy vasto, y en lo que sigue notaremos cualquier cosa que parezca especialmente digna de atención. Pero esta línea del argumento es tan fértil que deberemos pasar sobre muchos otros resultados que hemos descubierto, y sin duda muchos más permanecerán ocultos, esperando una

más amplia investigación. Finalmente, conviene notar que formas con determinante 0 están excluidas de los límites de nuestra investigación, a menos que específicamente mencionemos lo contrario.

Distribución de formas de un determinante dado en clases.

223.

Ya hemos mostrado (arts. 175, 195, 211) que, dado cualquier entero D (positivo o negativo) se puede asignar un número finito de formas F, F', F'', etc. con determinante D, tal que cada forma de determinante D sea propiamente equivalente a una, y sólo una, de éstas. Así todas las formas con determinante D (su número es infinito) pueden *clasificarse* según estas formas para componer una primera clase del conjunto de todas las formas propiamente equivalentes a la forma F; una segunda clase de formas que son propiamente equivalentes a la forma F', etc.

Una forma puede seleccionarse de cada una de las clases de formas con determinante dado D, y ésta será considerada como la *forma representante* de toda la clase. De por sí es enteramente arbitrario cuál forma es tomada de una clase dada, pero se debe preferir siempre la que parezca ser *más simple que las demás*. La simplicidad de una forma (a, b, c) ciertamente debe ser juzgada por el tamaño de los números a, b, c, y así la forma (a', b', c') se dice menos simple que (a, b, c) si $a' > a$, $b' > b$, $c' > c$. Pero esto no nos concede una determinación completa porque estaría ligeramente indefinido si e.g., escogemos $(17, 0, -45)$ o $(5, 0, -153)$ como la forma más simple. Sin embargo, muy a menudo sería ventajoso observar las siguientes normas.

I. Cuando el determinante D es negativo, se toman las formas reducidas en cada clase como las formas representantes; cuando dos formas en la misma clase son formas reducidas (ellas serán opuestas, art. 172), se toma aquélla cuyo término medio sea positivo.

II. Cuando el determinante D es positivo no cuadrado, se calcula el período de toda forma reducida contenida en la clase. Existirán o bien dos formas ambiguas o ninguna (art. 187).

1) En el primer caso sean (A, B, C) y (A', B', C') las formas ambiguas; y sean M y M' los residuos mínimos de los números B y B' según los módulos A y A' respectivamente (que se pueden tomar positivamente a menos que sean iguales a cero); finalmente, sean $\frac{D-M^2}{A} = N$, $\frac{D-M'^2}{A'} = N'$. Habiendo hecho esto, de las formas $(A, M, -N)$ y $(A', M', -N')$, tómese como forma representante aquélla que parezca ser la más simple. Para juzgar esto, la forma cuyo término medio es igual a

cero es la preferida; cuando el término medio es cero o es distinto de cero en ambas, la forma que posee el menor primer término se prefiere sobre la otra, y cuando los primeros términos sean iguales en tamaño pero con signos opuestos, aquélla con el signo positivo será la preferida.

2) Cuando no hay formas ambiguas en todo el período, se elige la forma cuyo primer término sea menor, sin importar el signo. Si ocurren dos formas en el mismo período, una con signo positivo y la otra con el mismo término con signo negativo, se deberá tomar la de signo positivo. Sea (A, B, C) la forma escogida y como en el caso anterior deducimos otra forma $(A, M, -N)$ a partir de ésta (esto es, tomando M como el menor residuo absoluto de B relativo al módulo A, y haciendo $N = \frac{D-M^2}{A}$); ésta será la forma representante.

Si sucediera que el mismo menor primer término A fuera común a varias formas del período, trátense todas estas formas de la manera que ya hemos delineado, y de las formas resultantes escójase como la forma representante aquélla que posea el menor término medio.

Así, e.g., para $D = 305$ uno de los períodos es: $(17, 4, -17)$, $(-17, 13, 8)$, $(8, 11, -23)$, $(-23, 12, 7)$, $(7, 16, -7)$, $(-7, 12, 23)$, $(23, 11, -8)$, $(-8, 13, 17)$, del cual se escoje la forma $(7, 16, -7)$, y entonces se deduce la forma representante $(7, 2, -43)$.

III. Cuando el determinante es un cuadrado positivo igual a k^2, se busca una forma reducida $(A, k, 0)$ en la clase bajo consideración y, si $A < k$ o $= k$, ésta es tomada como forma representante. Pero si $A > k$, tómese en su lugar la forma $(A - 2k, k, 0)$. El primer término será negativo, pero menor que k.

Ejemplo. De esta manera todas las formas del determinante -235 se distribuirán en dieciseis clases con los siguientes representantes: $(1, 0, 235)$, $(2, 1, 118)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(10, 5, 26)$, $(13, 5, 20)$, $(13, -5, 20)$ y otras ocho que son diferentes de las anteriores solamente en que poseen términos exteriores con signos opuestos: (-1, 0, -235), $(-2, 1, -118)$, etc.

Las formas con determinante 79 caen en seis clases con los siguientes representantes: $(1, 0, -79)$, $(3, 1, -26)$, $(3, -1, -26)$, $(-1, 0, 79)$, $(-3, 1, 26)$, $(-3, -1, 26)$.

224.

Mediante esta clasificación, formas que son propiamente equivalentes pueden separarse completamente de todas las demás. Dos formas con el mismo determinante serán propiamente equivalentes si ellas pertenecen a la misma clase; cualquier número

que sea representable por una de ellas será también representable por la otra; y si un número cualquiera M puede representarse por la primera forma de tal manera que los valores indeterminados sean primos entre sí, el mismo número podrá ser representado por la otra forma de la misma manera y, claro está, de manera que cada representación pertenezca al mismo valor de la expresión $\sqrt{D}$ (mod. M). Si, no obstante, dos formas pertenecen a diferentes clases, ellas no serán propiamente equivalentes; y si un número dado es representado por una de las formas, nada puede decirse con respecto a si éste es representable por la otra. Por otro lado, si el número M puede ser representado por una de éstas de tal manera que los valores de los indeterminados sean primos entre sí, podemos estar seguros inmediatamente que no existe representación similar del mismo número por otra forma que pertenezca al mismo valor de la expresión $\sqrt{D}$ (mod. M) (véanse arts. 167, 168).

Puede suceder, sin embargo, que dos formas F y F' que provienen de clases diferentes, K y K', sean impropiamente equivalentes, en este caso *toda* forma de una de las clases será impropiamente equivalente a *todas* las formas de la otra clase. Toda forma de K poseerá una forma opuesta en K' y las clases se llamarán *opuestas*. Así, en el primer ejemplo del artículo precedente, la tercera clase de formas con determinante -235 es opuesta a la cuarta, la sétima a la octava; en el segundo ejemplo, la segunda clase es opuesta a la tercera y la quinta a la sexta. Por esto, dadas dos formas cualesquiera de dos clases opuestas, cualquier número M que pueda representarse por una, también puede ser representado por la otra. Si en una esto sucede por valores primos entre sí de las indeterminadas, esto podrá suceder también en la otra pero de tal manera que estas dos representaciones correspondan a valores opuestos de la expresión $\sqrt{D}$ (mod. M). Además, las reglas dadas arriba para la elección de formas representantes están fundadas de modo que clases opuestas siempre dan origen a formas representantes opuestas.

Finalmente, existen clases que son *opuestas a sí mismas*. A saber, si alguna forma y su opuesta están contenidas en la misma clase, es fácil ver que todas las formas de esta clase son tanto propia como impropiamente equivalentes a alguna otra y que ellas tendrán todas sus opuestas en la clase. Cualquier clase tendrá esta propiedad si contiene una forma ambigua y, recíprocamente, una forma ambigua se encuentra en cualquier clase que es opuesta a sí misma (art. 163, 165). Por esto le llamaremos *clase ambigua*. Así, entre las clases con determinante -235 se encuentran ocho clases ambiguas. Sus formas representantes son $(1, 0, 235)$, $(2, 1, 118)$, $(5, 0, 47)$, $(10, 5, 26)$, $(-1, 0, -235)$, $(-2, 1, -118)$, $(-5, 0, -47)$, $(-10, 5, -26)$; entre las clases de formas con determinante 79 se encuentran dos con representantes: $(1, 0, -79)$

y $(-1, 0, 79)$. Pero si las formas representadas han sido determinadas de acuerdo con nuestras reglas, las clases ambiguas se pueden determinar a partir de ellas sin ningún problema. Esto es, para un determinante positivo no cuadrado una clase ambigua ciertamente corresponde a una forma representante ambigua (art. 194); para un determinante negativo la forma representante de una clase ambigua será ella misma ambigua o bien sus términos exteriores serán iguales (art. 172); finalmente, para un determinante positivo cuadrado, por el artículo 210 es fácil deducir si la forma representante es impropiamente equivalente a sí misma y así si la clase a la cual representa es ambigua.

225.

Nosotros demostramos arriba (art. 175) que para una forma (a, b, c) con determinante negativo los términos exteriores deben poseer el mismo signo y que éste será el mismo signo que el de los términos exteriores de cualquier otra forma equivalente a ésta. Si a y c son positivos, podremos llamar *positiva* a la forma (a, b, c), y diremos que la clase entera en la cual (a, b, c) está contenida, y la cual está compuesta sólo por formas positivas, es una *clase positiva*. Al contrario (a, b, c) será una *forma negativa* contenida en una *clase negativa* si a y c son negativos. Un número negativo no puede representarse por una forma positiva, ni un número positivo lo puede ser por una forma negativa. Si (a, b, c) es la forma representante de una clase positiva, $(-a, b, -c)$ será la forma representante de una clase negativa. Así se sigue que el número de clases positivas es igual al número de clases negativas, y tan pronto como conozcamos una conoceremos la otra. Por lo tanto, al investigar formas con determinante negativo es muy a menudo suficiente considerar clases positivas, ya que sus propiedades pueden ser fácilmente transferidas a clases negativas.

Pero esta distinción se cumple sólo para formas con determinante negativo; números positivos y negativos pueden representarse igualmente por formas con determinante positivo, así no es raro encontrar en este caso las dos formas (a, b, c) y $(-a, b, -c)$ en la misma clase.

Distribución de clases en órdenes.

226.

Llamamos *primitiva* a la forma (a, b, c) si los números a, b, c no poseen divisores en común; en otro caso la llamaremos *derivada* y, claro está, si el máximo

común divisor de a, b, c es igual a m, la forma (a, b, c) será la forma *derivada de la forma primitiva* $(\frac{a}{m}, \frac{b}{m}, \frac{c}{m})$. A partir de esta definición es obvio que cualquier forma cuyo determinante no es divisible por ningún cuadrado (excepto 1) es necesariamente primitiva. Además, por el artículo 161, si tenemos una forma primitiva en una clase arbitraria dada de formas con determinante D, todas las formas de esa clase serán primitivas; en este caso se dice que la clase misma es *primitiva*. Y es claro que, si cualquier forma F con determinante D se deriva de una forma primitiva f con determinante $\frac{D}{m^2}$, y si las clases en las cuales las formas F y f respectivamente están contenidas son K y k, todas las formas de la clase K serán formas derivadas de la clase primitiva k; en este caso diremos que la clase K es asimismo *derivada de la clase primitiva* k.

Si (a, b, c) es una forma primitiva y a y c no son ambos pares (i.e. o uno es impar o bien ambos son impares), entonces evidentemente no sólo a, b y c sino también a, $2b$ y c no poseen divisores comunes. En este caso la forma (a, b, c) se dice *propiamente primitiva* o simplemente una *forma propia*. Pero si (a, b, c) es una forma primitiva y los números a y c son ambos pares, obviamente los números a, $2b$ y c tendrán el divisor común 2 (este será también el máximo divisor) y (a, b, c) se llamará una *forma impropiamente primitiva* o simplemente una *forma impropia**). En este caso b será necesariamente impar (en otro caso (a, b, c) no sería una forma primitiva); por lo tanto tendremos $b^2 \equiv 1 \pmod 4$ y, como ac es divisible por 4, el determinante $b^2 - ac \equiv 1 \pmod 4$. Por lo que formas impropias corresponderán solamente a determinantes de la forma $4n + 1$ si son positivos o de la forma $-(4n+3)$ si son negativos. A partir del artículo 161 es obvio que si encontramos una forma propiamente primitiva en una clase dada, todas las formas de esta clase serán propiamente primitivas y que una clase que incluya una forma impropiamente primitiva estará compuesta solamente por formas impropiamente primitivas. Por ende, en el primer caso la clase se llamará *propiamente primitiva* o simplemente *propia*; y en el último caso *impropiamente primitiva* o *impropia*. Así, p. ej., entre las clases positivas de formas con determinante -235 existen seis propias con formas representantes $(1, 0, 235)$, $(4, 1, 59)$, $(4, -1, 59)$, $(5, 0, 47)$, $(13, 5, 20)$ y $(13, -5, 20)$ y el mismo número de negativas; y se encuentran dos clases impropias en cada una. Todas las clases de formas con determinante 79 (dado que ellas son de la forma $4n+3$) son propias.

---

*) Hemos escogido aquí los términos *propiamente* e *impropiamente* porque no hay otros más convenientes. Deseamos prevenir al lector de no buscar alguna conexión entre este caso y el del artículo 157 porque no existe ninguna. Pero ciertamente no se debería temer la ambigüedad.

Si la forma (a, b, c) se deriva de la forma primitiva $(\frac{a}{m}, \frac{b}{m}, \frac{c}{m})$ esta última puede ser o propiamente o bien impropiamente primitiva. En el primer caso m será también el máximo común divisor de los números a, $2b$, c; en el último el máximo común divisor será $2m$. A partir de esto podemos hacer una clara distinción entre una *forma derivada de una forma propiamente primitiva* y una *forma derivada de una forma impropiamente primitiva*; y además (ya que por el art. 161 todas las formas de una misma clase son las mismas en ese sentido) entre una *clase derivada de una clase propiamente primitiva* y una *clase derivada de una clase impropiamente primitiva*.

Por medio de estas distinciones hemos obtenido el primer principio fundamental sobre el cual podemos construir la noción de distribución de todas las clases de formas con un determinante dado en varios *órdenes*. Dadas dos representaciones (a, b, c) y (a', b', c'), las agruparemos en el *mismo orden* siempre que los números a, b y c tengan el mismo máximo común divisor que a', b' y c', y, a, $2b$ y c posean el mismo máximo común divisor que a', $2b'$ y c'; si una u otra de esas condiciones falla, las clases serán asignadas a *órdenes diferentes*. Es claro de inmediato que todas las clases propiamente primitivas constituirán un orden; y todas las clases impropiamente primitivas otro. Si m^2 es un cuadrado que divide al determinante D, las clases derivadas de las clases propiamente primitivas del determinante $\frac{D}{m^2}$ formarán un orden especial, y las clases derivadas de clases impropiamente primitivas del determinante $\frac{D}{m^2}$ formarán otro, etc. Si D es divisible por un no cuadrado (excepto 1), no habrá órdenes de clases derivadas, y así habrá o solamente un orden (cuando $D \equiv 2$ o 3 según módulo 4) que es un orden de clases propiamente primitivas, o dos órdenes (cuando $D \equiv 1 \pmod 4$), esto es, un orden de clases propiamente primitivas y un orden de clases impropiamente primitivas. No es difícil establecer la siguiente regla general con la ayuda de los principios del cálculo de combinaciones. Suponemos que $D = D' 2^{2\mu} a^{2\alpha} b^{2\beta} c^{2\gamma} \dots$ donde D' denota un factor no cuadrado y a, b, c, etc. son diferentes números primos impares (cualquier número puede reducirse a esta forma tomando $\mu = 0$ cuando D no es divisible por 4; y cuando D no es divisible por un cuadrado impar tomamos α, β, γ, etc. iguales a 0 o, lo que es la misma cosa, omitimos los factores $a^{2\alpha}$, $b^{2\beta}$, $c^{2\gamma}$, etc.); así habrá o

$$(\mu + 1)(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$$

órdenes cuando $D' \equiv 2$ ó $3 \pmod 4$; o

$$(\mu + 2)(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$$

órdenes cuando $D' \equiv 1 \pmod 4$. Pero no demostraremos esta regla, dado que no es difícil ni es necesaria aquí.

Ejemplo. 1. Para $D = 45 = 5 \cdot 3^2$ tenemos seis clases con representantes $(1, 0, -45)$, $(-1, 0, 45)$, $(2, 1, -22)$, $(-2, 1, 22)$, $(3, 0, -15)$, $(6, 3, -6)$. Estas se distribuyen en cuatro órdenes. El orden I incluye dos clases propias cuyas representantes son $(1, 0, 45)$ y $(-1, 0, 45)$; el orden II contendrá dos clases impropias cuyas representantes son $(2, 1, -22)$ y $(-2, 1, 22)$; el orden III contendrá una clase derivada de la clase propia del determinante 5, con representante $(3, 0, -15)$; el orden IV estará conformado por una clase derivada de una clase impropia del determinante 5 con representante $(6, 3, -6)$.

Ejemplo. 2. Las clases positivas del determinante $-99 = -11 \cdot 3^2$ se distribuirá en cuatro órdenes: el orden I incluirá las siguientes clases propiamente primitivas:*) $(1, 0, 99)$, $(4, 1, 25)$, $(4, -1, 25)$, $(5, 1, 20)$, $(5, -1, 20)$, $(9, 0, 11)$; el orden II contendrá las clases impropias $(2, 1, 50)$, $(10, 1, 10)$; el orden III contendrá las clases derivadas de las clases propias del determinante -11, a saber $(3, 0, 33)$, $(9, 3, 12)$, $(9, -3, 12)$; el orden IV, la clase derivada de las clases impropias del determinante -11, i.e., $(6, 3, 18)$. Clases negativas de este determinante pueden distribuirse en órdenes de exactamente la misma manera.

Observaremos que *clases opuestas son siempre asignadas al mismo orden.*

227.

De todos estos diferentes órdenes el orden de las clases propiamente primitivas merece especial atención. Para cada clase derivada obtenemos su origen de ciertas clases primitivas (con un determinante mínimo) y, considerando éstas, las propiedades de las clases se harán claras de inmediato. Mostraremos después que cualquier clase impropiamente primitiva se asocia o con una clase propiamente primitiva o con tres (con el mismo determinante). Además, para determinantes negativos, se puede omitir la consideración de clases negativas, dado que ellas siempre corresponderán a ciertas clases positivas. A fin de entender más plenamente la naturaleza de las clases propiamente primitivas, debemos primero explicar una cierta diferencia esencial según la cual el orden completo de clases propias puede subdividirse en varios *géneros.* Dado que todavía no hemos alcanzado este muy importante tema, lo trataremos desde el principio.

*) Usando, por brevedad, las formas representantes en lugar de sus clases.

La partición de órdenes en géneros.

228.

TEOREMA. *Existe una infinidad de números no divisibles por un número primo p dado, que pueden representarse por una forma propiamente primitiva.*

Demostración. Si la forma $F = ax^2 + 2bxy + cy^2$, es claro que p no puede ser divisor de los tres números a, $2b$, c. Ahora si a no es divisible por p, es claro que si elegimos un número no divisible por p para x , y para y un número que sea divisible por p, el valor de la forma F no será divisible por p; cuando c no es divisible por p ocurrirá lo mismo si damos a x un valor divisible por p y a y un valor que no sea divisible por p; finalmente, cuando ambos a y c son divisibles por p, y $2b$ no lo es, la forma F tendrá un valor no divisible por p si damos a ambos x y y valores que no sean divisibles por p. *Q. E. D.*

Es obvio que el teorema también es válido para formas que sean *impropiamente primitivas* mientras que no se tenga $p = 2$.

Dado que muchas condiciones de este tipo se pueden dar simultáneamente, tal como que el mismo número es divisible por ciertos números primos pero no por otros (véase art. 32), es fácil notar que los números x e y se pueden determinar de infinitas maneras, resultando que la forma primitiva $ax^2 + 2bxy + cy^2$ adquiera un valor que no es divisible por cualquier cantidad de números primos, excluyendo, sin embargo, el número 2 cuando la forma sea impropiamente primitiva. Así podemos proponer el teorema más generalmente: *Siempre se puede representar por medio de cualquier forma primitiva una infinidad de números que sean primos relativos a un número dado (el cual es impar cuando la forma es impropiamente primitiva).*

229.

TEOREMA. *Sea F una forma primitiva con determinante D y p un número primo que divide a D: entonces los números no divisibles por p que pueden representarse por la forma F son todos residuos cuadráticos de p o todos no residuos.*

Demostración. Sea $F = (a, b, c)$, y sean m y m' dos números cualesquiera no divisibles por p que pueden ser representados por la forma F; o sea

$$m = ag^2 + 2bgh + ch^2, \quad m' = ag'^2 + 2bg'h' + ch'^2$$

Entonces tendremos

$$mm' = [agg' + b(gh' + hg') + chh']^2 - D[gh' - hg']^2$$

y mm' será congruente a un cuadrado según el módulo D y así también según p; i.e., mm' será un residuo cuadrático de p. Se sigue por lo tanto que ambos m y m' son residuos cuadráticos de p, o que ambos no lo son. *Q. E. D.*

De la misma manera podemos demostrar que cuando el determinante D es divisible por 4, todos los números primos representables por F son o congruentes a 1 o congruentes a 3 (mod. 4). Esto es, el producto de dos de esos números siempre será un residuo cuadrático de 4 y por ende congruente a 1 (mod. 4); así ambos deben ser congruentes a 1 o ambos a 3.

Finalmente, cuando D es divisible por 8, el producto de dos números impares cualesquiera que pueden representarse por F será un residuo cuadrático de 8 y por tanto congruente a 1 (mod. 8). Así, en este caso los números impares representables por F serán todos congruentes a 1, o todos congruentes a 3, o todos congruentes a 5, o todos congruentes a 7 (mod. 8).

De este modo, p. ej., ya que el número 10 que es un no residuo de 7 se puede representar por la forma $(10, 3, 17)$, todos los números no divisibles por 7 que se pueden representar por esa forma serán no residuos de 7. Como -3 es representable por la forma $(-3, 1, 49)$ y es congruente a 1 (mod. 4), todos los números impares representables por esta forma serán congruentes a 1 (mod. 4).

Si fuese necesario para nuestros propósitos, podríamos demostrar fácilmente que los números representables por la forma F no guardan tal relación con números primos que no dividan a D. Ambos residuos y no residuos de un número primo que no divide a D se pueden representar igualmente por la forma F. Por el contrario, con respecto a los números 4 y 8 existe una cierta analogía, en otros casos también, que no podemos atrasar.

I. *Cuando el determinante D de la forma primitiva F es congruente a* 3 (mod. 4)*, todos los números impares representables por la forma F serán congruentes a* 1 *o todos congruentes a* 3 (mod. 4). En efecto, si m y m' son dos números representables por F, el producto mm' podrá reducirse a la forma $p^2 - Dq^2$ tal y como hicimos arriba. Cuando cada uno de los números m y m' es impar, uno de los números p o q es necesariamente par, y el otro impar, y por ende uno de los cuadrados p^2 o q^2 será congruente a 0 y el otro a 1 (mod. 4). Así $p^2 - Dq^2$ debe ser ciertamente congruente a 1 (mod. 4), y ambos m y m' deben ser congruentes a 1 o a 3 (mod. 4). Luego, p. ej., ningún número impar, más que aquéllos de la forma $4n + 1$, puede representarse por la forma $(10, 3, 17)$.

II. *Cuando el determinante D de la forma primitiva F es congruente a* 2 (mod. 8)*: todos los números impares representables por la forma F serán o*

congruentes en parte a 1 *y en parte a* 7*, o bien en parte a* 3 *y en parte a* 5 (mod. 8). En efecto, supongamos que m y m' son dos números impares representables por F cuyo producto mm' puede reducirse a la forma $p^2 - Dq^2$. Por lo que cuando ambos m y m' son impares, p debe ser impar (porque D es par) y así $p^2 \equiv 1 \pmod 8$; q^2 por lo tanto será congruente a 0, 1 o 4 y Dq^2 a 0 o a 2. Así $mm' = p^2 - Dq^2$ será congruente a 1 o a 7 (mod. 8); por eso, si m es congruente a 1 o a 7, m' será también congruente a 1 o a 7; y si m es congruente a 3 o a 5, m' será también congruente a 3 o a 5. Por ejemplo, todos los números impares representables por la forma $(3, 1, 5)$ son congruentes a 3 o a 5 (mod. 8), y ningún número de la forma $8n + 1$ u $8n + 7$ puede representarse por esta forma.

III. *Cuando el determinante D de una forma primitiva F es congruente a* 6 (mod. 8)*: los números impares que pueden representarse por esta forma son o todos congruentes a* 1 *y a* 3*, o todos congruentes a* 5 *y a* 7 (mod. 8). El lector puede desarrollar el argumento sin ningún problema. Es exactamente como el argumento anterior (II). Así, p. ej., para la forma $(5, 1, 7)$, solamente aquellos números impares que son congruentes a 5 o a 7 (mod. 8) pueden representarse.

230.

Por lo tanto todos los números que pueden representarse por una forma primitiva F dada con determinante D guardarán una estrecha relación con cada uno de los divisores primos de D (por el cual ellos no son divisibles). Y números impares que pueden representarse por la forma F guardarán también una estrecha relación con los números 4 y 8 en ciertos casos: a saber, con 4 siempre que D sea congruente a 0 o a 3 (mod. 4) y con 8 siempre que D sea congruente a 0, a 2 o a 6 (mod. 8)*). Llamaremos a este tipo de relación con cada uno de estos números el *carácter* o el *carácter particular* de la forma F, y expresaremos éste de la siguiente manera. Cuando solamente residuos cuadráticos de un número primo p pueden representarse por la forma F, asignaremos a ella el carácter Rp, en caso contrario asignaremos el carácter Np; similarmente escribiremos 1, 4 cuando ningún otro número puede representarse por la forma F excepto aquéllos que son congruentes a 1 (mod. 4). Es claro de inmediato cuáles caracteres se denotan por 3, 4; 1, 8; 3, 8; 5, 8 y 7, 8. Finalmente, si tenemos formas a través de las cuales solamente pueden representarse aquellos números impares que son congruentes a 1 o a 7 (mod. 8), les asignaremos a

*) Si el determinante es divisible por 8 se ignorará su relación con el número 4 pues en este caso ya se encuentra contenida en la relación con 8.

ellos el carácter 1 *y* 7, 8. Es obvio de inmediato que representamos por los caracteres 3 *y* 5, 8; 1 *y* 3, 8 ; 5 *y* 7, 8.

Los diferentes caracteres de una forma primitiva dada (a, b, c) con determinante D siempre se pueden conocer a partir de al menos uno de los números a o c (partiendo de que ambos son representables por tal forma). En efecto, siempre y cuando p sea un divisor primo de D, ciertamente uno de los números a o c, no será divisible por p; pues si ambos fueran divisibles por p, p dividiría también a b^2 $(= D+ac)$ y por lo tanto también a b; i.e. la forma (a, b, c) no sería primitiva. Similarmente, en aquellos casos en que la forma (a, b, c) posee una relación fija con el número 4 o el 8, al menos uno de los números a o c será impar, y podrá conocerse la relación de ese número. Así, p. ej., el carácter de la forma $(7, 0, 23)$ con respecto al número 23 puede inferirse a partir del número 7 como $N23$, y el carácter de la misma forma con respecto al número 7 puede deducirse a partir del número 23, a saber $R7$; finalmente, el carácter de esta forma con respecto al número 4, a saber 3, 4, puede hallarse a partir del número 7 o a partir del número 23.

Dado que todos los números que pueden representarse por una forma F contenida en una clase K son también representables por cualquier otra forma de la clase, queda manifiesto que los diferentes caracteres de la forma F se aplicarán a todas las demás formas de esta clase y por ende podemos considerar estos caracteres como representativos de toda la clase. Los caracteres individuales de una clase primitiva dada pueden entonces conocerse a partir de sus formas representantes. Clases opuestas poseerán siempre los mismos caracteres.

231.

El conjunto de *todos* los caracteres particulares de una clase o forma dada constituyen el carácter completo de esta forma o clase. Así, p. ej., el carácter completo de la forma $(10, 3, 17)$ o de la clase completa que ella representa será 1, 4; $N7$; $N23$. De manera análoga el carácter completo de la forma $(7, 1, -17)$ será 7, 8; $R3$; $N5$. Omitimos el carácter particular 3, 4 en este caso porque esta se halla contenida en el carácter 7, 8. A partir de estos resultados derivaremos una subdivisión del orden completo de clases propiamente primitivas (positivas cuando el determinante es negativo) de un determinante dado en muchos diferentes *géneros*, colocando todas las clases que poseen el mismo carácter completo en el mismo género, y en diferentes géneros aquéllos que poseen diferentes caracteres completos. Asignaremos a cada género aquéllos caracteres completos que poseen las clases contenidas en ellos. Así,

p. ej., para el determinante -161 tenemos 16 clases positivas propiamente primitivas que están distribuidas en 4 géneros de la siguiente manera:

Carácter	Formas representantes de las clases
1, 4; $R7$; $R23$	$(1,0,161)$, $(2,1,81)$, $(9,1,18)$, $(9,-1,18)$
1, 4; $N7$; $N23$	$(5,2,33)$, $(5,-2,33)$, $(10,3,17)$, $(10,-3,17)$
3, 4; $R7$; $N23$	$(7,0,23)$, $(11,2,15)$, $(11,-2,15)$, $(14,7,15)$
3, 4; $N7$; $R23$	$(3,1,54)$, $(3,-1,54)$, $(6,1,27)$, $(6,-1,27)$.

Se puede decir unas cuantas palabras con respecto a la cantidad de diferentes caracteres completos que son posibles *a priori*.

I. Cuando el determinante D es divisible por 8, con respecto al número 8 cuatro caracteres particulares son posibles; el número 4 no aportará ningún carácter en especial (véase el artículo precedente). Además, con respecto a cada divisor primo impar de D existirán dos caracteres; por lo tanto, si hay m de esos divisores, existirán en total 2^{m+2} diferentes caracteres completos (siendo $m = 0$ siempre que D sea potencia de 2).

II. Cuando el determinante D no es divisible por 8 pero sí es divisible por 4 y por m números primos impares, habrá en total 2^{m+1} caracteres completos diferentes.

III. Cuando el determinante es par y no divisible por 4, este será congruente a 2 o a 6 (mod. 8). En el primer caso existirán dos caracteres particulares con respecto al número 8, a saber 1 *y* 7, 8 y 3 *y* 5, 8; y el mismo número en el último caso. Por lo tanto, tomando el número de divisores primos impares de D igual a m, habrá en total 2^{m+1} caracteres completos diferentes.

IV. Cuando D es impar, será congruente a 1 o a 3 (mod. 4). En el segundo caso existirán dos diferentes caracteres con respecto al número 4, pero en el primer caso esta relación no formará parte del carácter completo. Así si definimos m como antes, en el primer caso existirán 2^m diferentes caracteres completos, en el último caso 2^{m+1}.

Pero hay que señalar bien que no se sigue *a priori* que siempre existirán tantos géneros como diferentes posibles caracteres. En nuestro ejemplo el número de clases o géneros es solamente la mitad de la cantidad posible. No existen clases positivas para los caracteres 1, 4; $R7$; $N23$ o 1, 4; $N7$; $R23$ o 3, 4; $R7$; $R23$ o 3, 4; $N7$; $N23$. Trataremos este importante tema plenamente más abajo.

A partir de ahora llamaremos a la forma $(1,0,-D)$, que es indudablemente la más simple de las formas con determinante D, la *forma principal*; y llamaremos a la clase completa en la cual ésta se encuentra la *clase principal*; y finalmente el género

completo en el cual se encuentra la clase principal se llamará *el género principal*. Por lo tanto, hay que distinguir claramente entre la forma principal, una forma de la clase principal, y una forma del género principal; y entre la clase principal y una clase del género principal. Siempre usaremos esta terminología, aún cuando quizás para un determinante en particular no exista otra clase más que la clase principal o ningún otro género más que el género principal. Esto sucede muy a menudo, p. ej., cuando D es un número primo positivo de la forma $4n + 1$.

232.

Aún cuando todo lo que se ha explicado sobre los caracteres de las formas fue con el propósito de encontrar una subdivisión para todo el orden de *clases positivas propiamente primitivas*, nada nos impide ir más lejos. Podemos aplicar las mismas reglas a formas y clases negativas o impropriamente primitivas, y bajo el mismo principio podemos subdividir en géneros tanto un orden positivo impropiamente primitivo, como un orden negativo propiamente primitivo, como un orden negativo impropiamente primitivo. Así pues, por ejemplo, después de que se ha subdividido el orden propiamente primitivo de formas de determinante 145 en los dos siguientes géneros:

$R5$, $R29$	$(1, 0, -145)$, $(5, 0, -29)$
$N5$, $N29$	$(3, 1, -48)$, $(3 - 1, -48)$

el orden impropiamente primitivo puede también ser subdividido en dos géneros:

$R5$, $R29$	$(4, 1, -36)$, $(4, -1, -36)$
$N5$, $N29$	$(2, 1, -72)$, $(10, 5, -12)$

o, tal como las clases positivas de las formas de determinante -129 se distribuyen en cuatro géneros:

1, 4; $R3$; $R43$	$(1, 0, 129)$, $(10, 1, 13)$, $(10, -1, 13)$
1, 4; $N3$; $N43$	$(2, 1, 65)$, $(5, 1, 26)$, $(5, -1, 26)$
3, 4; $R3$; $N43$	$(3, 0, 43)$, $(7, 2, 19)$, $(7, -2, 19)$
3, 4; $N3$; $R43$	$(6, 3, 23)$, $(11, 5, 14)$, $(11, -5, 14)$

las clases negativas también se pueden distribuir en cuatro órdenes:

3, 4; $N3$; $N43$	$(-1,0,-129)$, $(-10,1,-13)$, $(-10,-1,-13)$
3, 4; $R3$; $R43$	$(-2,1,-65)$, $(-5,1,-26)$, $(-5,-1,-26)$
1, 4; $N3$; $R43$	$(-3,0,-43)$, $(-7,2,-19)$, $(-7,-2,-19)$
1, 4; $R3$; $N43$	$(-6,3,-23)$, $(-11,5,-14)$, $(-11,-5,-14)$

Sin embargo, puesto que el sistema de clases negativas es siempre muy similar al sistema de clases positivas, resulta superfluo construirlo por aparte. Mostraremos luego cómo reducir un orden impropiamente primitivo a uno propiamente primitivo.

Finalmente, en cuanto a la subdivisión de órdenes obtenidos a partir de otros, no son necesarias reglas nuevas. Es así puesto que cualquiera de estos órdenes tiene origen en algún orden primitivo (con un determinante menor), y las clases de uno pueden relacionarse de manera natural con las clases del otro, y entonces es claro que la subdivisión de una de estas formas puede obtenerse a partir de la subdivisión de un orden primitivo.

233.

Si la forma (primitiva) $F = (a,b,c)$ es tal que se puede encontrar dos enteros g y h, tales que $g^2 \equiv a$, $gh \equiv b$, $h^2 \equiv c$ con respecto a un módulo dado m, diremos que la forma es un residuo cuadrático del número m, y que $gx + hy$ es un valor de la expresión $\sqrt{ax^2 + 2bxy + cy^2} \pmod{m}$ o simplemente que (g,h) es un valor de la expresión $\sqrt{(a,b,c)}$ o $\sqrt{F} \pmod{m}$. De manera más general, si el multiplicador M, primo relativo al módulo m es tal que tenemos

$$g^2 \equiv aM, \quad gh \equiv bM, \quad h^2 \equiv cM \pmod{m}$$

diremos que $M \cdot (a,b,c)$ o MF es un residuo cuadrático de m y que (g,h) es el valor de la expresión $\sqrt{M(a,b,c)}$ o $\sqrt{MF} \pmod{m}$. Por ejemplo, la forma $(3,1,54)$ es un residuo cuadrático de 23 y $(7,10)$ un valor de la expresión $\sqrt{(3,1,54)} \pmod{23}$; similarmente $(2,-4)$ es un valor de la expresión $\sqrt{5(10,3,17)} \pmod{23}$. El uso de estas definiciones se demostrará después. Anotaremos las siguientes proposiciones:

I. Si $M(a,b,c)$ es un residuo cuadrático del número m, m será un divisor del determinante de la forma (a,b,c). Pues si (g,h) es un valor de la expresión $\sqrt{M(a,b,c)} \pmod{m}$ es decir, si

$$g^2 \equiv aM, \quad gh \equiv bM, \quad h^2 \equiv cM \pmod{m}$$

tendremos $b^2M^2 - acM^2 \equiv 0$ o sea $(b^2 - ac)M^2$ es divisible por m. Pero, puesto que hemos supuesto que M y m son primos relativos, $b^2 - ac$ será divisible por m.

II. Si $M(a, b, c)$ es un residuo cuadrático de m, donde m es un número primo o una potencia p^μ de un número primo, el carácter particular de la forma (a, b, c) con respecto al número p será Rp o Np según M sea un residuo o no residuo de p. Esto se sigue inmediatamente del hecho de que ambos aM y cM son residuos de m o p, y que al menos uno de los números a y c no es divisible por p (art. 230).

Similarmente, si (con todo lo demás igual) $m = 4$, entonces 1, 4 ó 3, 4 será un carácter particular de la forma (a, b, c) según $M \equiv 1$ ó $M \equiv 3$; y si $m = 8$ o una potencia mayor del número 2, entonces, 1, 8; 3, 8; 5, 8; 7, 8 serán caracteres particulares de la forma (a, b, c) según $M \equiv 1;\ 3;\ 5;\ 7 \pmod 8$ respectivamente.

III. En cambio, suponga que m es un número primo o una potencia p^μ de un número primo impar y que es divisor del determinante $b^2 - ac$. Si M es un residuo o no de p según el carácter de la forma (a, b, c) respecto a p sea Rp o Np respectivamente, entonces $M(a, b, c)$ será un residuo cuadrático de m. Pues cuando a no es divisible por p, aM será un residuo de p y así también de m; por lo tanto, si g es un valor de la expresión $\sqrt{aM} \pmod m$, h un valor de la expresión $\frac{bg}{a} \pmod m$, tendremos $g^2 \equiv aM$, $ah \equiv bg$. Entonces

$$agh \equiv bg^2 \equiv abM \qquad \text{y} \quad gh \equiv bM$$

y finalmente

$$ah^2 \equiv bgh \equiv b^2M \equiv b^2M - (b^2 - ac)M \equiv acM$$

Así $h^2 \equiv cM$; i.e. (g, h) es un valor de la expresión $\sqrt{M(a, b, c)}$. Cuando a es divisible por m es de seguro que c no lo será. Entonces obviamente obtendremos el mismo resultado si h asume un valor de la expresión $\sqrt{cM} \pmod m$ y g un valor de la expresión $\frac{bh}{c} \pmod m$.

De manera similar se puede mostrar que si $m = 4$ y es divisor de $b^2 - ac$, y si el número M se toma $\equiv 1$ ó $\equiv 3$ según 1, 4 ó 3, 4 sea un carácter particular de la forma (a, b, c), entonces, $M(a, b, c)$ será un residuo cuadrático de m. Además, si $m = 8$ ó una potencia mayor de 2 y divisor de $b^2 - ac$, y si $M \equiv 1;\ 3;\ 5;\ 7 \pmod 8$ según el carácter particular de la forma (a, b, c) respecto al número 8; entonces $M(a, b, c)$ será un residuo cuadrático de m.

IV. Si el determinante de la forma (a, b, c) es $= D$ y $M(a, b, c)$ es un residuo cuadrático de D, a partir del número M pueden conocerse inmediatamente todos los caracteres particulares de la forma (a, b, c) respecto a cada uno de los divisores

primos impares de D y respecto al número 4 u 8 (si dividen a D). Entonces, por ejemplo, puesto que $3(20, 10, 27)$ es un residuo cuadrático de 440, es decir, que $(150, 9)$ es un valor de la expresión $\sqrt{3(20, 10, 27)}$ respecto al módulo 440 y $3N5$, $3R11$, los caracteres de la forma $(20, 10, 27)$ son 3, 8; $N5$; $R11$. Los caracteres particulares con respecto a los números 4 y 8, siempre que no sean divisores del determinante, son los únicos que no tienen una conexión necesaria con el número M.

V. En cambio, si el número M es primo relativo a D y contiene todos los caracteres particulares de la forma (a, b, c) (excepto por aquéllos respecto a los números 4 y 8 cuando no son divisores de D), entonces $M(a, b, c)$ será un residuo cuadrático de D. Pues, a partir de III es claro que si D se reduce a la forma $\pm A^\alpha B^\beta C^\gamma \ldots$ donde A, B, C, etc. son números primos distintos, $M(a, b, c)$ será un residuo cuadrático de cada uno de los A^α, B^β, C^γ, etc. Ahora supongamos que el valor de la expresión $\sqrt{M(a, b, c)}$ respecto al módulo A^α es $(\mathfrak{A}, \mathfrak{A}')$; respecto al módulo B^β es $(\mathfrak{B}, \mathfrak{B}')$; respecto al módulo C^γ es $(\mathfrak{C}, \mathfrak{C}')$ etc. Si los números g y h se determinan tales que $g \equiv \mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc; $h \equiv \mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$ etc. respecto a los módulos A^α, B^β, C^γ, etc. respectivamente (art. 32): es fácil ver que tendremos $g^2 \equiv aM$, $gh \equiv bM$, $h^2 \equiv cM$ respecto a cada uno de los módulos A^α, B^β, C^γ, etc. y, por lo tanto, también respecto al módulo D, que es su producto.

VI. Por esta razón números como M se llamarán *números característicos* de la forma (a, b, c). Muchos de estos números pueden encontrarse fácilmente mediante los métodos de V, una vez que se conocen todos los caracteres particulares de la forma. Los más sencillos se encontrarán por tanteo. Claramente, si M es un número característico de una forma primitiva de determinante D dado, todos los números congruentes a M respecto al módulo D serán números característicos de la misma forma. También es claro que formas de la misma clase o de diferentes clases del mismo género tienen los mismos números característicos. Como consecuencia, cualquier número característico de una forma dada también se puede asignar a toda la clase y a todo el género. Finalmente, 1 es siempre un número característico de cualquier forma, clase o género principal; es decir, toda forma de un género principal es un residuo de su determinante.

VII. Si (g, h) es un valor de la expresión $\sqrt{M(a, b, c)}$ (mod. m) y $g' \equiv g$ y $h' \equiv h$ (mod. m), entonces (g', h') también será un valor de la misma expresión. Tales valores se denominarán *equivalentes*. Sin embargo, si (g, h) y (g', h') son valores de la expresión $\sqrt{M(a, b, c)}$, pero no se cumple que $g' \equiv g$, $h' \equiv h$ (mod. m), se denominarán *diferentes*. Es claro que siempre que (g, h) sea un valor de una expresión como la anterior, $(-g, -h)$ también será un valor, y estos valores

siempre serán diferentes excepto cuando $m = 2$. También es fácil mostrar que una expresión $\sqrt{M(a,b,c)}$ (mod. m) no puede tener más que dos valores diferentes opuestos cuando m es un número primo impar, una potencia de un número primo impar ó $= 4$; sin embargo, cuando $m = 8$ ó una potencia mayor de 2, habrá cuatro en total. Entonces, a partir de VI vemos fácilmente que si el determinante D de la forma (a,b,c) es $= \pm 2^{\mu} A^{\alpha} B^{\beta} \ldots$ donde A, B, etc. son n números primos impares diferentes en total, y M es un número característico de la forma; entonces habrá, en total, 2^n ó 2^{n+1} ó 2^{n+2} valores diferentes de la expresión $\sqrt{M(a,b,c)}$ (mod. D) según μ sea < 2 ó $= 2$ ó > 2. Entonces, por ejemplo, hay 16 valores de la expresión $\sqrt{7(12,6,-17)}$ (mod. 240), a saber $(\pm 18, \mp 11)$, $(\pm 18, \pm 29)$, $(\pm 18, \mp 91)$, $(\pm 18, \pm 109)$, $(\pm 78, \pm 19)$, $(\pm 78, \pm 59)$, $(\pm 78, \mp 61)$, $(\pm 78, \mp 101)$. Para abreviar, y puesto que no es particularmente importante para lo que sigue, omitiremos una demostración más detallada.

VIII. Finalmente observamos que si el determinante de dos formas equivalentes (a,b,c) y (a',b',c') es D, el número característico es M y la primera se puede transformar en la segunda mediante la sustitución α, β, γ, δ; entonces, a partir de cualquier valor (g,h) de la expresión $\sqrt{M(a,b,c)}$ se obtiene un valor (g',h') de la expresión $\sqrt{M(a',b',c')}$, a saber $(\alpha g + \gamma h, \beta g + \delta h)$. El lector puede demostrar esto fácilmente.

Sobre la composición de formas.

234.

Ahora que hemos explicado la distribución de formas entre clases, géneros y órdenes, y las propiedades generales que resultan de estas distinciones, pasaremos a otro tema muy importante, la *composición* de formas. Hasta el momento, nadie ha considerado este punto. Antes de iniciar la discusión enunciaremos el siguiente lema para no interrumpir, más adelante, la continuidad de nuestra demostración.

LEMA: *Suponga que tenemos cuatro series de enteros.*

$$a,\ a',\ a'',\ \ldots a^n; \quad b,\ b',\ b'',\ \ldots b^n; \quad c,\ c',\ c'',\ \ldots c^n; \quad d,\ d',\ d'',\ \ldots d^n$$

donde cada serie tiene el mismo número $(n+1)$ *de términos y están ordenados tal que*

$$cd' - dc', \quad cd'' - dc'' \text{ etc.}, \quad c'd'' - d'c'' \text{ etc., etc.}$$

son respectivamente

$$= k(ab' - ba'), \quad k(ab'' - ba'') \text{ etc.}, \quad k(a'b'' - b'a'') \text{ etc., etc.}$$

o en general

$$c^\lambda d^\mu - d^\lambda c^\mu = k(a^\lambda b^\mu - b^\lambda a^\mu)$$

*Aquí k es un entero dado; λ y μ son dos enteros distintos cualesquiera entre 0 y n inclusive, con μ el mayor de los dos**). Además, no debe haber un divisor común entre todos los $a^\lambda b^\mu - b^\lambda a^\mu$. Bajo estas condiciones, se pueden encontrar cuatro enteros α, β, γ y δ tales que

$$\begin{array}{lll} \alpha a + \beta b = c, & \alpha a' + \beta b' = c', & \alpha a'' + \beta b'' = c'' \text{ etc.} \\ \gamma a + \delta b = d, & \gamma a' + \delta b' = d', & \gamma a'' + \delta b'' = d'' \text{ etc.} \end{array}$$

o en general

$$\alpha a^\nu + \beta b^\nu = c^\nu, \quad \gamma a^\nu + \delta b^\nu = d^\nu$$

y tenemos

$$\alpha\delta - \beta\gamma = k$$

Puesto que por hipótesis los números $ab' - ba'$, $ab'' - ba''$, etc. $a'b'' - b'a''$ etc. (el número de ellos será $= \frac{1}{2}(n+1)n$) no tienen un divisor común, podemos encontrar la misma cantidad de enteros (diferentes) tal que si multiplicamos el primer conjunto por el segundo respectivamente, la suma de los productos será $= 1$ (art. 40). Designaremos estos multiplicadores por $(0,1)$, $(0,2)$ etc., $(1,2)$ etc. o en general el multiplicador de $a^\lambda b^\mu - b^\lambda a^\mu$ por (λ, μ) y

$$\sum(\lambda,\ \mu)(a^\lambda b^\mu - b^\lambda a^\mu) = 1$$

(Mediante la letra $\sum$ indicamos la suma de todos los valores de la expresión cuando le damos sucesivamente a λ y a μ, todos los valores diferentes entre 0 y n y tal que $\mu > \lambda$). Ahora si se pone

$$\begin{array}{ll} \sum(\lambda,\mu)(c^\lambda b^\mu - b^\lambda c^\mu) = \alpha, & \sum(\lambda,\mu)(a^\lambda c^\mu - c^\lambda a^\mu) = \beta \\ \sum(\lambda,\mu)(d^\lambda b^\mu - b^\lambda d^\mu) = \gamma, & \sum(\lambda,\mu)(a^\lambda d^\mu - d^\lambda a^\mu) = \delta \end{array}$$

estos números α, β, γ y δ tienen las propiedades deseadas.

---

*) Tomando a como a^0, b como b^0 etc. Pero es claro que la misma ecuación es válida cuando $\lambda = \mu$ ó $\lambda > \mu$.

Demostración. I. Si ν es cualquier entero entre 0 y n, tenemos

$$\begin{aligned}\alpha a^\nu + \beta b^\nu &= \sum (\lambda,\mu)(c^\lambda b^\mu a^\nu - b^\lambda c^\mu a^\nu + a^\lambda c^\mu b^\nu - c^\lambda a^\mu b^\nu)\\ &= \frac{1}{k}\sum (\lambda,\mu)(c^\lambda d^\mu c^\nu - d^\lambda c^\mu c^\nu)\\ &= \frac{1}{k}c^\nu \sum (\lambda,\mu)(c^\lambda d^\mu - d^\lambda c^\mu)\\ &= c^\nu \sum (\lambda,\mu)(a^\lambda b^\mu - b^\lambda a^\mu) = c^\nu\end{aligned}$$

Y mediante un cálculo similar se demuestra

$$\gamma a^\nu + \delta b^\nu = d^\nu. \quad Q.\ E.\ P.$$

II. Entonces, puesto que

$$c^\lambda = \alpha a^\lambda + \beta b^\lambda, \qquad c^\mu = \alpha a^\mu + \beta b^\mu$$

se tiene

$$c^\lambda b^\mu - b^\lambda c^\mu = \alpha(a^\lambda b^\mu - b^\lambda a^\mu)$$

y similarmente

$$\begin{aligned}a^\lambda c^\mu - c^\lambda a^\mu &= \beta(a^\lambda b^\mu - b^\lambda a^\mu)\\ d^\lambda b^\mu - b^\lambda d^\mu &= \gamma(a^\lambda b^\mu - b^\lambda a^\mu)\\ a^\lambda d^\mu - d^\lambda a^\mu &= \delta(a^\lambda b^\mu - b^\lambda a^\mu)\end{aligned}$$

A partir de estas fórmulas pueden obtenerse los valores de α, β, γ y δ mucho más fácilmente, siempre y cuando λ y μ sean escogidos tales que $a^\lambda b^\mu - b^\lambda a^\mu$ no sea 0. Esto de seguro se puede lograr, ya que por hipótesis no hay un divisor común de todos los $a^\lambda b^\mu - b^\lambda a^\mu$ y por lo tanto todos no pueden ser 0. A partir de estas mismas ecuaciones, si multiplicamos la primera por la cuarta, la segunda por la tercera y restamos, obtenemos

$$(\alpha\delta - \beta\gamma)(a^\lambda b^\mu - b^\lambda a^\mu)^2 = (a^\lambda b^\mu - b^\lambda a^\mu)(c^\lambda d^\mu - d^\lambda c^\mu) = k(a^\lambda b^\mu - b^\lambda a^\mu)^2$$

y necesariamente entonces

$$\alpha\delta - \beta\gamma = k. \quad Q.\ E.\ S.$$

235.

Si la forma $AX^2 + 2BXY + CY^2 \ldots F$ se transforma en el producto de dos formas

$$ax^2 + 2bxy + cy^2 \ldots f, \quad \text{y} \quad a'x'^2 + 2b'x'y' + c'y'^2 \ldots f'$$

mediante la sustitución

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

(para abreviar, en lo que sigue expresaremos esta situación de la siguiente manera: Si F se transforma en ff' mediante la sustitución p, p', p'', p'''; q, q', q'', q'''*)), diremos simplemente que la forma F es *transformable* en ff'. Si además se construye esta transformación de tal manera que los seis números

$$pq' - qp',\ pq'' - qp'',\ pq''' - qp''',\ p'q'' - q'p'',\ p'q''' - q'p''',\ p''q''' - q''p'''$$

no tienen un divisor común, llamaremos a F una forma *compuesta* de las formas f y f'.

Iniciaremos esta discusión con la suposición más general de que la forma F se transforma en ff' mediante la sustitución p, p', p'', p'''; q, q', q'', q''' y descubriremos qué es lo que deducimos de ésto. Claramente las nueve ecuaciones siguientes son completamente equivalentes a esta suposición (i.e. cuando estas ecuaciones se cumplen F será transformada, mediante las sustituciones dadas, en ff', y vice-versa):

$$Ap^2 + 2Bpq + Cq^2 = aa' \qquad [1]$$
$$Ap'^2 + 2Bp'q' + Cq'^2 = ac' \qquad [2]$$
$$Ap''^2 + 2Bp''q'' + Cq''^2 = ca' \qquad [3]$$
$$Ap'''^2 + 2Bp'''q''' + Cq'''^2 = cc' \qquad [4]$$
$$App' + B(pq' + qp') + Cqq' = ab' \qquad [5]$$
$$App'' + B(pq'' + qp'') + Cqq'' = ba' \qquad [6]$$
$$Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc' \qquad [7]$$
$$Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb' \qquad [8]$$
$$A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') + C(qq''' + q'q'') = 2bb' \qquad [9]$$

*) En esta expresión debemos poner mucho cuidado en el orden de los coeficientes p, p', etc. y de las formas f y f'. Es fácil ver que si el orden de las formas f y f' se cambia tal que la primera se convierte en la segunda, los coeficientes p' y q' deben intercambiarse con p'' y q'' y los otros deben permanecer iguales.

Sean D, d y d' los determinantes de las formas F, f y f' respectivamente; y sean M, m y m' los máximos comunes divisores de los números A, $2B$, C; a, $2b$, c; a', $2b'$, c', respectivamente (suponemos que todos estos números son positivos). Además sean los seis enteros $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$ determinados de modo que

$$\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m, \qquad \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$$

Finalmente desígnense los números

$$pq' - qp', \quad pq'' - qp'', \quad pq''' - qp''', \quad p'q'' - q'p'', \quad p'q''' - q'p''', \quad p''q''' - q''p'''$$

por P, Q, R, S, T, U respectivamente y sea k su máximo común divisor tomado positivamente. Ahora, haciendo

$$App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta \qquad [10]$$

de la ecuación [9] obtenemos

$$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta \qquad [11]$$

A partir de esas once ecuaciones desarrollamos las siguientes*):

$$DP^2 = d'a^2 \qquad [12]$$
$$DP(R-S) = 2d'ab \qquad [13]$$
$$DPU = d'ac - (\Delta^2 - dd') \qquad [14]$$
$$D(R-S)^2 = 4d'b^2 + 2(\Delta^2 - dd') \qquad [15]$$
$$D(R-S)U = 2d'bc \qquad [16]$$
$$DU^2 = d'c^2 \qquad [17]$$
$$DQ^2 = da'^2 \qquad [18]$$
$$DQ(R+S) = 2da'b' \qquad [19]$$
$$DQT = da'c' - (\Delta^2 - dd') \qquad [20]$$
$$D(R+S)^2 = 4db'^2 + 2(\Delta^2 - dd') \qquad [21]$$
$$D(R+S)T = 2db'c' \qquad [22]$$
$$DT^2 = dc'^2 \qquad [23]$$

*) El origen de estas ecuaciones es como sigue: [12] de $[5]^2 - [1][2]$; [13] de $[5][9] - [1][7] - [2][6]$; [14] de $[10][11] - [6][7]$; [15] de $2[5][8] + [10]^2 + [11]^2 - [1][4] - [2][3] - 2[6][7]$; [16] de $[8][9] - [3][7] - [4][6]$; [17] de $[8]^2 - [3][4]$. Podemos deducir las seis ecuaciones restantes por medio de los mismos esquemas, si reemplazamos las ecuaciones [3], [6], [8] por las ecuaciones [2], [5], [7] respectivamente y dejamos [1], [4], [9], [10], [11] tal como aparecen. Por ejemplo, la ecuación [18] viene de $[6]^2 - [1][3]$, etc.

Y a partir de ellas deducimos las dos siguientes:

$$0 = 2d'a^2(\Delta^2 - dd')$$
$$0 = (\Delta^2 - dd')^2 - 2d'ac(\Delta^2 - dd')$$

la primera a partir de las ecuaciones $[12][15] - [13]^2$, la segunda a partir de las ecuaciones $[14]^2 - [12][17]$; y es fácil notar que $\Delta^2 - dd' = 0$ tanto si a es igual a cero como si no lo es*). Supongamos que se ha cancelado $\Delta^2 - dd'$ de las ecuaciones [14], [15], [20] y [21].

Ahora

$$\mathfrak{A}P + \mathfrak{B}(R - S) + \mathfrak{C}U = mn'$$
$$\mathfrak{A}'Q + \mathfrak{B}'(R + S) + \mathfrak{C}'T = m'n$$

(donde n y n' pueden ser fracciones siempre que mn' y $m'n$ sean enteros). A partir de las ecuaciones [12]-[17] se deduce que

$$Dm^2n'^2 = d'(\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c)^2 = d'm^2$$

y de las ecuaciones [18]-[23]

$$Dm'^2n^2 = d'(\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c')^2 = dm'^2$$

Tenemos entonces $d = Dn^2$, $d' = Dn'^2$ y a partir de esto obtenemos una PRIMERA CONCLUSIÓN: *Los cocientes de los determinantes de las formas F, f y f' necesariamente son cuadrados*; y una SEGUNDA: *D siempre divide a los números dm'^2 y $d'm^2$.* Entonces es claro que D, d y d' tienen el mismo signo y que ninguna forma puede transformarse en el producto ff' si su determinante es mayor que el máximo común divisor de dm'^2 y $d'm^2$.

Multiplicamos las ecuaciones [12], [13], [14] por $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ respectivamente y similarmente a las ecuaciones [13], [15], [16] y [14], [16], [17] por los mismos números y sumamos los tres productos. Divida la suma por Dmn', escribiendo Dn'^2 en vez de d'. Entonces se obtiene

$$P = an', \quad R - S = 2bn', \quad U = cn'$$

*) Esta manera de derivar la ecuación $\Delta^2 = dd'$ es suficiente para nuestros propósitos actuales. Podríamos haber deducido directamente de las ecuaciones [1] a [11] que $0 = (\Delta^2 - dd')^2$. Este podría haber sido un análisis más elegante pero demasiado prolongado en este punto.

De manera semejante, multiplicando las ecuaciones [18], [19], [20] y [19], [21], [22] y [20], [22], [23] por $\mathfrak{A}'$, $\mathfrak{B}'$ y $\mathfrak{C}'$ resulta

$$Q = a'n, \quad R + S = 2b'n, \quad T = c'n$$

A partir de esto obtenemos una TERCERA CONCLUSIÓN: *Los números a, $2b$, y c son proporcionales a los números P, $R-S$ y U. Si la razón del primero al segundo se toma como 1 a n', n' será la raíz cuadrada de $\frac{d'}{D}$; de la misma manera los números a', $2b'$ y c' son proporcionales a los números Q, $R+S$ y T y si tomamos la razón como 1 a n, n será la raíz cuadrada de $\frac{d}{D}$.*

Ahora, las cantidades n y n' pueden ser o raíces positivas o raíces negativas de $\frac{d}{D}$ y $\frac{d'}{D'}$, así haremos una distinción que puede parecer estéril a primera vista, pero su uso quedará claro en lo que sigue. Diremos que en la transformación de la forma F en ff' la forma f se toma *directamente* cuando n es positivo e *inversamente* cuando n es negativo; de manera análoga f' se toma directamente o inversamente de acuerdo con que n' sea positivo o negativo. Dada la condición de que k sea igual a 1, se dice que la forma F está compuesta de las dos formas f y f' directamente *o* de las dos inversamente *o* de f directamente y de f' inversamente *o* de f inversamente y de f' directamente según que n y n' sean ambos positivos o ambos negativos o que el primero sea positivo y el segundo negativo o el primero negativo y el segundo positivo. Es fácil notar que estas relaciones no dependen del orden en que se hayan tomado las formas (véase la primera nota de este artículo).

Notamos además que k, el máximo común divisor de los números P, Q, R, S, T y U, divide a los números mn' y $m'n$ (como queda claro a partir de los valores que establecimos más arriba). Por tanto el cuadrado k^2 divide a $m^2n'^2$ y m'^2n^2, y Dk^2 divide a $d'm^2$ y $d'm'^2$. Pero recíprocamente, todo divisor común de mn' y $m'n$ divide a k. Sea e un divisor tal: evidentemente este dividirá a an', $2bn'$, cn', $a'n$, $2b'n$ y $c'n$; i.e., a los números P, $R-S$, U, Q, $R+S$ y T y también a $2R$ y $2S$. Ahora si $\frac{2R}{e}$ es un número impar, $\frac{2S}{e}$ también debe ser impar (pues la suma y la diferencia son pares) y el producto también deberá ser impar. Este producto es igual a $\frac{4}{e^2}(b'^2n^2 - b^2n'^2) = \frac{4}{e^2}(d'n^2 + a'c'n^2 - dn'^2 - acn'^2) = \frac{4}{e^2}(a'c'n^2 - acn'^2)$ y por tanto par, porque e divide a $a'n$, $c'n$, an' y cn'. Así $\frac{2R}{e}$ es necesariamente par y ambos R y S son divisibles por e. Ya que e divide a los seis P, Q, R, S, T y U, también dividirá a k, su máximo común divisor. *Q. E. D.* Concluimos que k es el máximo común divisor de los números mn' y $m'n$, y *Dk^2 será el máximo común divisor de los números dm'^2, $d'm^2$.* Esta es nuestra CUARTA CONCLUSIÓN. Ahora es claro

que siempre que F se componga de f y f', D será el máximo común divisor de los números dm'^2 y $d'm^2$ y vice versa. Estas propiedades pudieron también utilizarse como la definición de las formas compuestas. Por ende, la forma que está compuesta de las formas f y f', posee el máximo determinante posible de todas las formas que son transformables en el producto ff'.

Antes de que continuemos más adelante, definiremos primero el valor de Δ más exactamente. Mostramos que $\Delta = \sqrt{dd'} = \sqrt{D^2n^2n'^2}$, pero no se ha determinado aún su *signo*. Para tal propósito deducimos a partir de las ecuaciones fundamentales [1] a [11] que $DPQ = \Delta aa'$ (obtenemos esto a partir de [5][6] − [1][11]). Así $Daa'nn' = \Delta aa'$, y a menos que uno de los números a o a' sea igual a 0, tenemos $\Delta = Dnn'$. Exactamente de la misma forma, a partir de las ecuaciones fundamentales podemos deducir otras ocho en las cuales tenemos Dnn' a la izquierda y Δ en la derecha multiplicados por $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$ y cc'*). Ahora, dado que no todos a, $2b$ y c ni todos a', $2b'$ y c' pueden ser iguales a 0, en todos los casos $\Delta = Dnn'$ y Δ posee el mismo signo que D, d y d' o el opuesto, según que n y n' posean el mismo signo o signos diferentes.

Observamos que los números aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$, cc', $2bb' + 2\Delta$ y $2bb' - 2\Delta$ son todos divisibles por mm'. Esto es obvio para los primeros nueve números. Para los otros dos podemos mostrar, como hicimos al principio, que R y S son divisibles por e. Es claro que $4bb' + 4\Delta$ y $4bb' - 4\Delta$ son divisibles por mm' (dado que $4\Delta = \sqrt{16dd'}$ y $4d$ es divisible por m^2, $4d'$ por m'^2, y así $16dd'$ por $m^2m'^2$ y 4Δ por mm') y que la diferencia de los cocientes es par. Es fácil demostrar que el producto de los cocientes es par, y así que cada cociente es par y que $2bb' + 2\Delta$, $2bb' - 2\Delta$ son divisibles por mm'.

Ahora a partir de las once ecuaciones fundamentales derivamos las seis siguientes:

$$
\begin{aligned}
AP^2 &= aa'q'^2 - 2ab'qq' + ac'q^2 \\
AQ^2 &= aa'q''^2 - 2ba'qq'' + ca'q^2 \\
AR^2 &= aa'q'''^2 - 2(bb' + \Delta)qq''' + cc'q^2 \\
AS^2 &= ac'q''^2 - 2(bb' - \Delta)q'q'' + ca'q'^2 \\
AT^2 &= ac'q'''^2 - 2bc'q'q''' + cc'q'^2 \\
AU^2 &= ca'q'''^2 - 2cb'q''q''' + cc'q''^2
\end{aligned}
$$

*) El lector puede verificar este análisis fácilmente. Lo omitimos en aras de la brevedad.

Se sigue por lo tanto que todos AP^2, AQ^2, etc. son divisibles por mm' y dado que k^2 es el máximo común divisor de los números P^2, Q^2, R^2, etc., Ak^2 será también divisible por mm'. Si sustituimos por a, $2b$, c, a', $2b'$ y c' sus valores $\frac{P}{n'}$, etc. o $\frac{1}{n'}(pq' - qp')$, etc., ellos podrían cambiarse por otras seis ecuaciones en las cuales tendremos, en el lado derecho, productos de la cantidad $\frac{1}{nn'}(q'q'' - qq''')$ por P^2, Q^2, R^2, etc. Dejaremos estos sencillos cálculos al lector. Se sigue (puesto que no todo P^2, Q^2, etc. $= 0$) que $Ann' = q'q'' - qq'''$.

Similarmente, a partir de las ecuaciones fundamentales podemos obtener otras seis ecuaciones que difieren de las anteriores en que se reemplazan A y q, q', q'', q''' por C y p, p', p'', p''' respectivamente. Para abreviar omitimos los detalles. Finalmente, de modo semejante se sigue que Ck^2 es divisible por mm' y $Cnn' = p'p'' - pp'''$.

Nuevamente podemos deducir otras seis ecuaciones a partir de los mismos datos:

$$\begin{aligned}
BP^2 &= -aa'p'q' + ab'(pq' + qp') - ac'pq \\
BQ^2 &= -aa'p''q'' + ba'(pq'' + qp'') - ca'pq \\
BR^2 &= -aa'p'''q''' + (bb' + \Delta)(pq''' + qp''') - cc'pq \\
BS^2 &= -ac'p''q'' + (bb' - \Delta)(p'q'' + q'p'') - ca'p'q' \\
BT^2 &= -ac'p'''q''' + bc'(p'q''' + q'p''') - cc'p'q' \\
BU^2 &= -ca'p'''q''' + cb'(p''q''' + q''p''') - cc'p''q''
\end{aligned}$$

y a partir de esto, como en el caso anterior, concluimos que $2Bk^2$ es divisible por mm' y $2Bnn' = pq''' + qp''' - p'q'' - q'p''$.

Ahora, puesto que Ak^2, $2Bk^2$ y Ck^2 son divisibles por mm', es fácil ver que Mk^2 también debe ser divisible por mm'. De las ecuaciones fundamentales sabemos que M es divisor de aa', $2ab'$, ac', $2ba'$, $4bb'$, $2bc'$, ca', $2cb'$ y cc' y por lo tanto también de am', $2bm'$ y cm' (los cuales son los máximos comunes divisores de los primeros, segundos y últimos tres respectivamente); y finalmente que también es divisor de mm', el cual es el máximo común divisor de todos éstos. Por lo tanto, en este caso, donde la forma F está compuesta por las formas f, f', eso es $k = 1$, M necesariamente $= mm'$. Esta es nuestra Quinta Conclusión.

Si designamos el máximo común divisor de los números A, B y C por $\mathfrak{M}$, será $= M$ (cuando la forma F es propiamente primitiva o se obtiene a partir de una forma propiamente primitiva) ó $= \frac{1}{2}M$ (cuando F es impropiamente primitiva o se obtiene a partir de una forma impropiamente primitiva); similarmente, si designamos los máximos comunes divisores de los números a, b y c; a', b' y c' por $\mathfrak{m}$ y $\mathfrak{m}'$ respectivamente, $\mathfrak{m}$ será $= m$ ó $= \frac{1}{2}m$ y $\mathfrak{m}'$ será $= m'$ ó $= \frac{1}{2}m'$. Ahora, es claro

que $\mathfrak{m}^2$ es divisor de d, $\mathfrak{m}'^2$ es divisor de d'. Por lo tanto $\mathfrak{m}^2\mathfrak{m}'^2$ es divisor de dd' o de Δ^2, y $\mathfrak{m}\mathfrak{m}'$ es divisor de Δ. De las últimas seis ecuaciones para BP^2 etc. se sigue que $\mathfrak{m}\mathfrak{m}'$ es divisor de Bk^2 y (puesto que también es divisor de Ak^2 y de Ck^2) de $\mathfrak{M}k^2$. Por lo tanto, cada vez que F esté compuesta por f y f', $\mathfrak{m}\mathfrak{m}'$ será divisor de $\mathfrak{M}$. Y cuando ambos f y f' son propiamente primitivas u obtenidas a partir de formas propiamente primitivas, o $\mathfrak{m}\mathfrak{m}' = mm' = M$, entonces $\mathfrak{M} = M$ ó F es una forma similar. Pero, si bajo las mismas condiciones una o ambas formas f y f' son impropiamente primitivas u obtenidas a partir de formas impropiamente primitivas, entonces (si la forma f por ejemplo lo es) a partir de las ecuaciones fundamentales se sigue que aa', $2ab'$, ac', ba', $2bb'$, bc', ca', $2cb'$, cc' son divisibles por $\mathfrak{M}$ y así también am', bm', cm' y $\mathfrak{m}m' = \frac{1}{2}mm' = \frac{1}{2}M$; en este caso $\mathfrak{M} = \frac{1}{2}M$ y la forma F es impropiamente primitiva u obtenida a partir de una forma impropiamente primitiva. Esta es nuestra SEXTA CONCLUSIÓN.

Finalmente observamos que, si *se supone* que las siguientes nueve ecuaciones son verdaderas,

$$\begin{gathered} an' = P, \quad 2bn' = R - S, \quad cn' = U \\ a'n = Q, \quad 2b'n = R + S, \quad c'n = T \\ Ann' = q'q'' - qq''', \quad 2Bnn' = pq''' + qp''' - p'q'' - q'p'', \quad Cnn' = p'p'' - pp''' \end{gathered}$$

(en lo que sigue, designaremos estas condiciones por Ω, ya que las retomaremos frecuentemente) entonces, tomando n y n' como incógnitas pero ninguna $= 0$, encontramos mediante una sustitución sencilla que las ecuaciones fundamentales [1] a [9] son necesariamente verdaderas, o sea, que la forma (A, B, C) será transformada en el producto de las formas $(a, b, c)(a', b', c')$ mediante la sustitución p, p', p'', p'''; q, q', q'', q'''. También tendremos

$$b^2 - ac = n^2(B^2 - AC), \qquad b'^2 - a'c' = n'^2(B^2 - AC)$$

El cálculo, que sería demasiado largo para exponerlo aquí, lo dejamos al lector.

236.

PROBLEMA. *Dadas dos formas cuyos determinantes son iguales o por lo menos difieren por factores cuadrados: encontrar una forma compuesta por estas dos.*

Solución. Sean $(a,b,c)\ldots f$ y $(a',b',c')\ldots f'$ las formas iniciales; d y d' sus determinantes; m y m' los máximos comunes divisores de los números a, $2b$, c; a', $2b'$, c' respectivamente; D el máximo común divisor de los números dm'^2 y $d'm^2$ tomados con el mismo signo que d y d'. Entonces $\frac{dm'^2}{D}$ y $\frac{d'm^2}{D}$ serán números positivos primos relativos y su producto será un cuadrado; por lo tanto cada uno de ellos será un cuadrado (art. 21). Así pues, $\sqrt{\frac{d}{D}}$ y $\sqrt{\frac{d'}{D}}$ serán cantidades racionales que dejaremos ser $= n$, n' y escogeremos para n un valor positivo o negativo dependiendo de si la forma f debe entrar directa o inversamente en la composición. De manera similar determinaremos el signo de n' según la manera en la cual la forma f' debe entrar en la composición. Entonces mn' y $m'n$ serán enteros primos entre sí; n y n' pueden ser fracciones. Ahora observamos que an', cn', $a'n$, $c'n$, $bn'+b'n$ y $bn'-b'n$ son enteros. Esto es obvio para los primeros cuatro (puesto que $an' = \frac{a}{m}mn'$ etc.); para los últimos dos lo probamos tal como se hizo en el último artículo para probar que R y S son divisibles por e.

Tomemos ahora cuatro enteros $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$ y $\mathfrak{Q}'''$ arbitrarios con sólo una condición, que las cuatro cantidades a la izquierda de las siguientes ecuaciones (I) no sean todas $= 0$. Ahora, considérense las ecuaciones:

$$\begin{aligned}
\mathfrak{Q}'an' + \mathfrak{Q}''a'n + \mathfrak{Q}'''(bn'+b'n) &= \mu q \\
-\mathfrak{Q}an' + \mathfrak{Q}'''c'n - \mathfrak{Q}''(bn'-b'n) &= \mu q' \\
\mathfrak{Q}'''cn' - \mathfrak{Q}a'n + \mathfrak{Q}'(bn'-b'n) &= \mu q'' \\
-\mathfrak{Q}''cn' - \mathfrak{Q}'c'n - \mathfrak{Q}(bn'+b'n) &= \mu q'''
\end{aligned} \qquad (I)$$

tales que q, q', q'' y q''' son enteros sin un divisor común. Esto se puede lograr tomando para μ el máximo común divisor de los cuatro números que están a la izquierda de las ecuaciones. Ahora, según el artículo 40 podemos encontrar cuatro enteros $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$ y $\mathfrak{P}'''$ tales que

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

Una vez logrado ésto, determínense los números p, p', p'' y p''' mediante las siguientes ecuaciones:

$$\begin{aligned}
\mathfrak{P}'an' + \mathfrak{P}''a'n + \mathfrak{P}'''(bn'+b'n) &= p \\
-\mathfrak{P}an' + \mathfrak{P}'''c'n - \mathfrak{P}''(bn'-b'n) &= p' \\
\mathfrak{P}'''cn' - \mathfrak{P}a'n + \mathfrak{P}'(bn'-b'n) &= p'' \\
-\mathfrak{P}''cn' - \mathfrak{P}'c'n' - \mathfrak{P}(bn'+b'n) &= p'''
\end{aligned} \qquad (II)$$

Ahora se hacen las siguientes sustituciones:

$$q'q'' - qq''' = Ann', \quad pq''' + qp''' - p'q'' - q'p'' = 2Bnn', \quad p'p'' - pp''' = Cnn'$$

Entonces A, B y C serán enteros y la forma $(A, B, C) \ldots F$ será compuesta por las formas f y f'.

Demostración. I. A partir de (I) obtenemos las siguientes cuatro ecuaciones:

$$\begin{aligned} 0 &= q'cn' - q''c'n - q'''(bn' - b'n) \\ 0 &= qcn' + q'''a'n - q''(bn' + b'n) \\ 0 &= q'''an' + qc'n - q'(bn' + b'n) \\ 0 &= q''an' - q'a'n - q(bn' - b'n) \end{aligned} \qquad (III)$$

II. Ahora supongamos que los enteros $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, $\mathfrak{N}$, $\mathfrak{N}'$ se determinan de modo que

$$\begin{aligned} \mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c &= m \\ \mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' &= m' \\ \mathfrak{N}m'n + \mathfrak{N}'mn' &= 1 \end{aligned}$$

Entonces tendremos

$$\mathfrak{A}a\mathfrak{N}'n' + 2\mathfrak{B}b\mathfrak{N}'n' + \mathfrak{C}c\mathfrak{N}'n' + \mathfrak{A}'a'\mathfrak{N}n + 2\mathfrak{B}'b'\mathfrak{N}n + \mathfrak{C}'c'\mathfrak{N}n = 1$$

A partir de esto y las ecuaciones (III), si dejamos que

$$\begin{aligned} -q'\mathfrak{A}\mathfrak{N}' - q''\mathfrak{A}'\mathfrak{N} - q'''(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q} \\ q\mathfrak{A}\mathfrak{N}' - q'''\mathfrak{C}'\mathfrak{N} + q''(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}' \\ -q'''\mathfrak{C}\mathfrak{N}' + q\mathfrak{A}'\mathfrak{N} - q'(\mathfrak{B}\mathfrak{N}' - \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}'' \\ q''\mathfrak{C}\mathfrak{N}' + q'\mathfrak{C}'\mathfrak{N} + q(\mathfrak{B}\mathfrak{N}' + \mathfrak{B}'\mathfrak{N}) &= \mathfrak{q}''' \end{aligned}$$

obtendremos

$$\begin{aligned} \mathfrak{q}'an' + \mathfrak{q}''a'n + \mathfrak{q}'''(bn' + b'n) &= q \\ -\mathfrak{q}an' + \mathfrak{q}'''c'n - \mathfrak{q}''(bn' - b'n) &= q' \\ \mathfrak{q}'''cn' - \mathfrak{q}a'n + \mathfrak{q}'(bn' - b'n) &= q'' \\ -\mathfrak{q}''cn' - \mathfrak{q}'c'n - \mathfrak{q}(bn' + b'n) &= q''' \end{aligned} \qquad (IV)$$

Cuando $\mu = 1$ estas ecuaciones son innecesarias y se pueden utilizar las ecuaciones (I), que son enteramente análogas, en su lugar. Ahora, a partir de las ecuaciones (II) y (IV) determinamos los valores de Ann', $2Bnn'$ y Cnn' (i.e. de los números $q'q'' - qq'''$ etc.) y suprimimos los valores que se anulan entre sí, y encontramos que los términos diferentes son productos de enteros por nn', dn'^2 o $d'n^2$. Además, todos los términos de $2Bnn'$ contienen el factor 2. Concluimos que A, B y C son enteros (porque $dn'^2 = d'n^2$ y por lo tanto $\frac{dn'^2}{nn'} = d'\frac{n^2}{nn'} = \sqrt{dd'}$ son enteros). *Q. E. P.*

III. Si tomamos los valores de p, p', p'' y p''' de (II), utilizamos las ecuaciones (III) y la siguiente:

$$\mathfrak{P}q + \mathfrak{P}'q' + \mathfrak{P}''q'' + \mathfrak{P}'''q''' = 1$$

encontramos que

$$\begin{array}{llll} pq' - qp' = an', & pq''' - qp''' - p'q'' + q'p'' = 2bn', & p''q''' - q''p''' = cn' \\ pq'' - qp'' = a'n, & pq''' - qp''' + p'q'' - q'p'' = 2b'n, & p'q''' - q'p''' = c'n \end{array}$$

Estas ecuaciones son idénticas a las primeras seis (Ω) del artículo anterior. Las tres restantes son parte de la hipótesis. Por lo tanto (final del mismo artículo) la forma F se transformará en ff' mediante la sustitución p, p', p'', p'''; q, q', q'', q'''; su determinante será $= D$, o sea, será igual al máximo común divisor de los números dm'^2 y $d'm^2$. Según la cuarta conclusión del artículo anterior esto significa que F está compuesta por f y f', *Q. E. S.* Y finalmente se sabe que F se compone de f y f' según la forma prescrita puesto que los signos de n y n' se determinaron correctamente al comienzo.

237.

TEOREMA. *Si la forma F es transformable en el producto de dos formas f y f', y la forma f' implica la forma f'', entonces F también será transformable en el producto de las formas f y f''.*

Demostración. Para las formas F, f y f' todas las notaciones del artículo 235 se mantienen; sea $f'' = (a'', b'', c'')$ y sea f' transformado en f'' mediante la sustitución α, β, γ, δ. Entonces F se transformará en ff'' mediante la sustitución

$$\begin{array}{llll} \alpha p + \gamma p', & \beta p + \delta p', & \alpha p'' + \gamma p''', & \beta p'' + \delta p''' \\ \alpha q + \gamma q', & \beta q + \delta q', & \alpha q'' + \gamma q''', & \beta q'' + \delta q''' \end{array} \quad Q.\ E.\ D.$$

Para abreviar designaremos estos coeficientes como sigue:

$$\alpha p + \gamma p', \quad \beta p + \delta p' \text{ etc.} = \mathfrak{P}, \mathfrak{P}', \mathfrak{P}'', \mathfrak{P}'''; \ \mathfrak{Q}, \mathfrak{Q}', \mathfrak{Q}'', \mathfrak{Q}'''$$

y sea el número $\alpha\delta - \beta\gamma = e$. A partir de las ecuaciones Ω, artículo 235, es fácil ver que

$$\begin{aligned}
\mathfrak{P}\mathfrak{Q}' - \mathfrak{Q}\mathfrak{P}' &= an'e \\
\mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' + \mathfrak{Q}'\mathfrak{P}'' &= 2bn'e \\
\mathfrak{P}''\mathfrak{Q}''' - \mathfrak{Q}''\mathfrak{P}''' &= cn'e \\
\mathfrak{P}\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{P}'' = \alpha^2 a'n + 2\alpha\gamma b'n + \gamma^2 c'n &= a''n \\
\mathfrak{P}\mathfrak{Q}''' - \mathfrak{Q}\mathfrak{P}''' + \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2b''n \\
\mathfrak{P}'\mathfrak{Q}''' - \mathfrak{Q}'\mathfrak{P}''' &= c''n \\
\mathfrak{Q}'\mathfrak{Q}'' - \mathfrak{Q}\mathfrak{Q}''' &= Ann'e \\
\mathfrak{P}\mathfrak{Q}''' + \mathfrak{Q}\mathfrak{P}''' - \mathfrak{P}'\mathfrak{Q}'' - \mathfrak{Q}'\mathfrak{P}'' &= 2Bnn'e \\
\mathfrak{P}'\mathfrak{P}'' - \mathfrak{P}\mathfrak{P}''' &= Cnn'e
\end{aligned}$$

Ahora, si designamos el determinante de la forma f'' por d'', e será una raíz cuadrada de $\frac{d''}{d'}$, positiva o negativa según la forma f' implica la forma f'' propia o impropiamente. Así pues $n'e$ será una raíz cuadrada de $\frac{d''}{D}$; y las nueve ecuaciones anteriores serán completamente análogas a las ecuaciones Ω del artículo 235. La forma f se tomará en la transformación de la forma F en ff'' de manera idéntica a como se tomó en la transformación de la forma F en ff'. La forma f'' en la primera debe tomarse como se tomó f' en la segunda si f' implica f'' propiamente. Si f' implica f'' impropiamente, debe tomarse de manera opuesta.

238.

TEOREMA. *Si la forma F está contenida en la forma F' y es transformable en el producto de las formas f y f'; entonces la forma F' será transformable en el mismo producto.*

Demostración. Si para las formas F, f y f' se retiene la misma notación que en el caso anterior y si se supone además que la forma F' se transforma en F mediante la sustitución α, β, γ, δ, es fácil ver que, mediante la sustitución

$$\begin{aligned}
&\alpha p + \beta q, \quad \alpha p' + \beta q', \quad \alpha p'' + \beta q'', \quad \alpha p''' + \beta q''' \\
&\gamma p + \delta q, \quad \gamma p' + \delta q', \quad \gamma p'' + \delta q'', \quad \gamma p''' + \delta q'''
\end{aligned}$$

F' se convierte en lo mismo que F mediante la sustitución p, p', p'', p'''; q, q', q'', q''' y por lo tanto a través de esta transformación F' se transforma en ff'. *Q. E. D.*

Mediante un cálculo similar al del artículo anterior también es posible comprobar que F' es transformable en ff' de la misma manera que F, cuando F' implica F propiamente. Pero cuando F está contenida impropiamente en F' las transformaciones de las formas F y F' en ff' serán opuestas respecto a cada una de las formas f y f'; eso es, si una forma aparece en una de las transformaciones directamente, aparecerá en la otra de manera inversa.

Si combinamos este teorema con el del artículo anterior obtendremos la siguiente generalización. *Si la forma F es transformable en el producto ff', si las formas f y f' implican las formas g y g' respectivamente, y si la forma F está contenida en la forma G: entonces G será transformable en el producto gg'.* En efecto, según el teorema de éste artículo G es transformable en ff' y así según el teorema anterior en fg' y así también en gg'. También es claro que, si todas las tres formas f, f' y G implican las formas g, g' y F propiamente, G será transformable en gg' con respecto a las formas g y g' de igual manera que F en ff' con respecto a las formas f y f'. Lo mismo es cierto si las tres implicaciones son impropias. Si una de las implicaciones es diferente de las otras dos, es igualmente fácil determinar *cómo* G es transformable en gg'.

Si las formas F, f y f' son equivalentes a las formas G, g y g' respectivamente, los segundos tendrán los mismos determinantes que los primeros. Y m y m' serán para g y g' los mismos que para f y f' (art. 161). Así pues, según la cuarta conclusión del artículo 235 se deduce que G está *compuesta* por g y g' si F está compuesta por f y f'; y de hecho la forma g entrará en la primera composición de igual manera que f lo hace en la segunda, siempre y cuando F sea equivalente a G de la misma manera que f lo es a g y vice versa. Similarmente g' debe tomarse en la primera composición de manera igual u opuesta a como se tomó f' en la segunda, según la equivalencia de las formas f' y g' sea similar o no a la equivalencia de las formas F y G.

239.

Teorema. *Si la forma F está compuesta por las formas f y f', cualquier otra forma que sea transformable en el producto ff' de la misma manera que F, implicará a F propiamente.*

Demostración. Si mantenemos la notación del artículo 235 para las formas F, f y f', las ecuaciones Ω también tendrán lugar aquí. Supongamos que la forma

$F' = (A', B', C')$ cuyo determinante $= D'$ se transforma en el producto ff' mediante la sustitución $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, $\mathfrak{p}'''$; $\mathfrak{q}$, $\mathfrak{q}'$, $\mathfrak{q}''$, $\mathfrak{q}'''$. Designemos los números

$$\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}', \quad \mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'', \quad \mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''', \quad \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'', \quad \mathfrak{p}'\mathfrak{q}''' - \mathfrak{q}'\mathfrak{p}''', \quad \mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}'''$$

respectivamente por

$$P', \quad Q', \quad R', \quad S', \quad T', \quad U'$$

Entonces se tendrán nueve ecuaciones que son completamente similares a las de Ω, a saber

$$\begin{gathered} P' = a\mathfrak{n}', \quad R' - S' = 2b\mathfrak{n}', \quad U' = c\mathfrak{n}' \\ Q' = a'\mathfrak{n}, \quad R' + S' = 2b'\mathfrak{n}, \quad T' = c'\mathfrak{n} \\ q'q'' - qq''' = A'\mathfrak{n}\mathfrak{n}', \quad \mathfrak{p}\mathfrak{q}''' + \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'' = 2B'\mathfrak{n}\mathfrak{n}', \quad \mathfrak{p}'\mathfrak{p}'' - \mathfrak{p}\mathfrak{p}''' = C'\mathfrak{n}\mathfrak{n}' \end{gathered}$$

Designaremos estas ecuaciones por Ω'. Las cantidades $\mathfrak{n}$ y $\mathfrak{n}'$ son, en este caso, las raíces cuadradas de $\frac{d}{D'}$ y $\frac{d'}{D'}$, y tienen el mismo signo que n y n' respectivamente; entonces, si tomamos la raíz cuadrada positiva de $\frac{D}{D'}$ (será un entero) y lo hacemos $= k$, tendremos $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$. Entonces, a partir de las primeras seis ecuaciones de Ω y Ω' obtenemos

$$\begin{gathered} P' = kP, \quad Q' = kQ, \quad R' = kR \\ S' = kS, \quad T' = kT, \quad U' = kU \end{gathered}$$

Según el lema del artículo 234 podrán encontrarse cuatro enteros α, β, γ, δ tales que

$$\begin{gathered} \alpha p + \beta q = \mathfrak{p}, \quad \gamma p + \delta q = \mathfrak{q} \\ \alpha p' + \beta q' = \mathfrak{p}', \quad \gamma p' + \delta q' = \mathfrak{q}' \text{ etc.} \end{gathered}$$

y

$$\alpha\delta - \beta\gamma = k$$

Sustituyendo estos valores de $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{p}'$, $\mathfrak{q}'$, etc. en las últimas tres ecuaciones de Ω' y utilizando las ecuaciones $\mathfrak{n} = kn$, $\mathfrak{n}' = kn'$ y las últimas tres ecuaciones de Ω encontramos que

$$\begin{gathered} A'\alpha^2 + 2B'\alpha\gamma + C'\gamma^2 = A \\ A'\alpha\beta + B'(\alpha\delta + \beta\gamma) + C'\gamma\delta = B \\ A'\beta^2 + 2B'\beta\delta + C'\delta^2 = C \end{gathered}$$

Por lo tanto, mediante la sustitución α, β, γ, δ (que será propia puesto que $\alpha\delta - \beta\gamma = k$ es positivo) F' se transformará en F i.e. implicará la forma F propiamente. *Q. E. D.*

Por lo tanto si F' está compuesta por las formas f y f' (de la misma manera que F), las formas F y F' tendrán el mismo determinante y serán propiamente equivalentes. De manera más general, si la forma G está compuesta por las formas g y g' de la misma manera que F está compuesta por las formas f y f' respectivamente y las formas g y g' son propiamente equivalentes a f y f': entonces las formas F y G son propiamente equivalentes.

Puesto que este caso, donde ambas formas a componer entran directamente en la composición, es el más sencillo y los otros se pueden reducir fácilmente a él, sólo consideraremos éste en lo que sigue. Entonces si alguna forma se dice estar compuesta por otras dos, se debe interpretar siempre como si estuviera propiamente compuesta de cada una de ellas*). La misma restricción quedará implícita cuando se dice que una forma es transformable en un producto de otras dos.

240.

Teorema. *Si la forma F está compuesta de las formas f y f'; la forma $\mathfrak{F}$ de F y f''; la forma F' de f y f''; la forma $\mathfrak{F}'$ de F' y f': entonces las formas $\mathfrak{F}$ y $\mathfrak{F}'$ serán propiamente equivalentes.*

Demostración. I. Sea

$$\begin{aligned}
f &= ax^2 + 2bxy + cy^2 \\
f' &= a'x'^2 + 2b'x'y' + c'y'^2 \\
f'' &= a''x''^2 + 2b''x''y'' + c''y''^2 \\
F &= AX^2 + 2BXY + CY^2 \\
F' &= A'X'^2 + 2B'X'Y' + C'Y'^2 \\
\mathfrak{F} &= \mathfrak{A}\mathfrak{X}^2 + 2\mathfrak{B}\mathfrak{X}\mathfrak{Y} + \mathfrak{C}\mathfrak{Y}^2 \\
\mathfrak{F}' &= \mathfrak{A}'\mathfrak{X}'^2 + 2\mathfrak{B}'\mathfrak{X}'\mathfrak{Y}' + \mathfrak{C}'\mathfrak{Y}'^2
\end{aligned}$$

y sean d, d', d'', D, D', $\mathfrak{D}$ y $\mathfrak{D}'$ los determinantes de las siete formas respectivamente. Todos tendrán los mismos signos y diferirán por factores cuadrados. Además, sea m el

*) Tal como en una composición de razones (la cual es muy similar a la composición de formas) normalmente entendemos que las razones son tomadas directamente a menos que se indique lo contrario.

máximo común divisor de los números a, $2b$, c y sean m', m'' y M con el mismo sentido respecto a las formas f', f'' y F. Entonces a partir de la cuarta conclusión del artículo 235, D será el máximo común divisor de los números dm'^2, $d'm^2$; Dm''^2 el máximo común divisor de los números $dm'^2m''^2$, $dm^2m''^2$; $M = mm'$; $\mathfrak{D}$ el máximo común divisor de los números Dm''^2, $d''M^2$ o de los números Dm''^2, $d''m^2m'^2$. Concluimos que $\mathfrak{D}$ es el máximo común divisor de los tres números $dm'^2m''^2$, $d'm^2m''^2$, $d''m^2m'^2$. Por razones similares $\mathfrak{D}'$ será el máximo común divisor de los mismos tres números. Entonces, puesto que $\mathfrak{D}$ y $\mathfrak{D}'$ tienen el mismo signo, $\mathfrak{D} = \mathfrak{D}'$ y las formas $\mathfrak{F}$ y $\mathfrak{F}'$ tendrán el mismo determinante.

II. Ahora, sea F que se transforma en ff' mediante la sustitución

$$X = pxx' + p'xy' + p''yx' + p'''yy'$$
$$Y = qxx' + q'xy' + q''yx' + q'''yy'$$

y $\mathfrak{F}$ en Ff' mediante la sustitución

$$\mathfrak{X} = \mathfrak{p}Xx'' + \mathfrak{p}'Xy'' + \mathfrak{p}''Yx'' + \mathfrak{p}'''Yy''$$
$$\mathfrak{Y} = \mathfrak{q}Xx'' + \mathfrak{q}'Xy'' + \mathfrak{q}''Yx'' + \mathfrak{q}'''Yy''$$

y designemos las raíces positivas de $\frac{d}{D}$, $\frac{d'}{D}$, $\frac{D}{\mathfrak{D}}$, $\frac{d''}{\mathfrak{D}}$ por n, n', $\mathfrak{N}$, $\mathfrak{n}''$. Entonces, según el artículo 235 habrá 18 ecuaciones, la mitad de las cuales pertenecen a la transformación de la forma F en ff' y la otra mitad a la transformación de la forma $\mathfrak{F}$ en Ff''. La primera de ellas será $pq' - qp' = an'$. Las demás se podrán generar de la misma manera, pero para abreviar, las omitiremos aquí. Note que las cantidades n, n', $\mathfrak{N}$, $\mathfrak{n}''$ serán racionales pero no necesariamente enteros.

III. Si los valores de X e Y se sustituyen en los valores de $\mathfrak{X}$ e $\mathfrak{Y}$ obtenemos un resultado de la forma:

$$\begin{aligned}\mathfrak{X} = \quad & (1)xx'x'' + (2)xx'y'' + (3)xy'x'' + (4)xy'y'' \\ & + (5)yx'x'' + (6)yx'y'' + (7)yy'x'' + (8)yy'y'' \\ \mathfrak{Y} = \quad & (9)xx'x'' + (10)xx'y'' + (11)xy'x'' + (12)xy'y'' \\ & + (13)yx'x'' + (14)yx'y'' + (15)yy'x'' + (16)yy'y''\end{aligned}$$

Obviamente, mediante esta sustitución $\mathfrak{F}$ se transformará en el producto $ff'f''$. El coeficiente (1) será $= p\mathfrak{p} + q\mathfrak{p}''$ y el lector podrá desarrollar los quince valores restantes. Designaremos el número $(1)(10) - (2)(9)$ por $(1,2)$, el número $(1)(11) - (3)(9)$ por $(1,3)$ y en general $(g)(8+h) - (h)(8+g)$ por (g,h) donde g y h son enteros diferentes

entre 1 y 16 con h el mayor de ellos*); de esta manera tenemos 28 símbolos en total. Ahora si designamos las raíces cuadradas positivas de $\frac{d}{\mathfrak{D}}$ y $\frac{d'}{\mathfrak{D}}$ por $\mathfrak{n}$ y $\mathfrak{n}'$ (serán $= n\mathfrak{N}$ y $n'\mathfrak{N}$) tendremos las siguientes 28 ecuaciones:

$$
\begin{aligned}
(1,2) &= aa'\mathfrak{n}'' & (3,5) &= a''b'\mathfrak{n} - a''b\mathfrak{n}' \\
(1,3) &= aa''\mathfrak{n}' & (3,6) &= bb'\mathfrak{n}'' + b'b''\mathfrak{n} - bb''\mathfrak{n}' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' \\
(1,4) &= ab'\mathfrak{n}'' + ab''\mathfrak{n}' & (3,7) &= a''c'\mathfrak{n} \\
(1,5) &= a'a''\mathfrak{n} & (3,8) &= bc'\mathfrak{n}'' + b''c'\mathfrak{n} \\
(1,6) &= a'b\mathfrak{n}'' + a'b''\mathfrak{n} & (4,5) &= b'b''\mathfrak{n} - bb'\mathfrak{n}'' - bb''\mathfrak{n}' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' \\
(1,7) &= a''b\mathfrak{n}' + a''b'\mathfrak{n} & (4,6) &= b'c''\mathfrak{n} - bc''\mathfrak{n}' \\
(1,8) &= bb'\mathfrak{n}'' + bb''\mathfrak{n}' + b'b''\mathfrak{n} + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' & (4,7) &= b''c'\mathfrak{n} - bc'\mathfrak{n}'' \\
(2,3) &= ab''\mathfrak{n}' - ab'\mathfrak{n}'' & (4,8) &= c'c''\mathfrak{n} \\
(2,4) &= ac''\mathfrak{n}' & (5,6) &= ca'\mathfrak{n}'' \\
(2,5) &= a'b''\mathfrak{n} - a'b\mathfrak{n}'' & (5,7) &= ca''\mathfrak{n}' \\
(2,6) &= a'c''\mathfrak{n} & (5,8) &= b'c\mathfrak{n}'' + b''c\mathfrak{n}' \\
(2,7) &= bb''\mathfrak{n}' + b'b''\mathfrak{n} - bb'\mathfrak{n}'' - \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'' & (6,7) &= b''c\mathfrak{n}' - b'c\mathfrak{n}'' \\
(2,8) &= bc''\mathfrak{n}' + b'c''\mathfrak{n} & (6,8) &= cc''\mathfrak{n}' \\
(3,4) &= ac'\mathfrak{n}'' & (7,8) &= cc'\mathfrak{n}''
\end{aligned}
$$

Designaremos estas ecuaciones por Φ, y tendremos otras nueve:

$$
\begin{aligned}
(10)(11) - (9)(12) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(1)(12) - (2)(11) - (3)(10) + (4)(9) &= 2a\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(2)(3) - (1)(4) &= a\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
-(9)(16) + (10)(15) + (11)(14) - (12)(13) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
\left.\begin{aligned}(1)(16) - (2)(15) - (3)(14) + (4)(13) \\ + (5)(12) - (6)(11) - (7)(10) + (8)(9)\end{aligned}\right\} &= 4b\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
-(1)(8) + (2)(7) + (3)(6) - (4)(5) &= 2b\mathfrak{n}'\mathfrak{n}''\mathfrak{C} \\
(14)(15) - (13)(16) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{A} \\
(5)(16) - (6)(15) - (7)(14) + (8)(13) &= 2c\mathfrak{n}'\mathfrak{n}''\mathfrak{B} \\
(6)(7) - (5)(8) &= c\mathfrak{n}'\mathfrak{n}''\mathfrak{C}
\end{aligned}
$$

*) El significado actual de estos símbolos no debe confundirse con su significado en el artículo 234 pues los números que se expresan mediante estos signos *aquí* corresponden más bien a los del artículo 234 que son multiplicados por números denotados por símbolos similares.

a las que designaremos por Ψ*).

IV. Tomaría demasiado tiempo deducir todas las 37 ecuaciones, nos conformaremos con establecer algunas de ellas como un modelo para las demás.

1) Tenemos

$$\begin{aligned}(1,2) &= (1)(10) - (2)(9)\\ &= (\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}')p^2 + (\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''' - \mathfrak{p}'\mathfrak{q}'' + \mathfrak{q}'\mathfrak{p}'')pq + (\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}''')q^2\\ &= \mathfrak{n}''(Ap^2 + 2Bpq + Cq^2) = \mathfrak{n}''aa'\end{aligned}$$

que es la primera ecuación.

2) Tenemos

$$(1,3) = (1)(11) - (3)(9) = (\mathfrak{p}\mathfrak{q}'' - \mathfrak{q}\mathfrak{p}'')(pq' - qp') = a''\mathfrak{N}an' = aa''\mathfrak{n}'$$

la segunda ecuación

3) Y tenemos

$$\begin{aligned}(1,8) &= (1)(16) - (8)(9)\\ &= (\mathfrak{p}\mathfrak{q}' - \mathfrak{q}\mathfrak{p}')pp''' + (\mathfrak{p}\mathfrak{q}''' - \mathfrak{q}\mathfrak{p}''')pq''' - (\mathfrak{p}'\mathfrak{q}'' - \mathfrak{q}'\mathfrak{p}'')qp''' + (\mathfrak{p}''\mathfrak{q}''' - \mathfrak{q}''\mathfrak{p}''')qq'''\\ &= \mathfrak{n}''(App''' + B(pq''' + qp''') + Cqq''') + b''\mathfrak{N}(pq''' - qp''')\\ &= \mathfrak{n}''(bb' + \sqrt{dd'}) + b''\mathfrak{N}(b'n + bn') \quad \dagger)\\ &= \mathfrak{n}''bb' + \mathfrak{n}'bb'' + \mathfrak{n}b'b'' + \mathfrak{D}\mathfrak{n}\mathfrak{n}'\mathfrak{n}'',\end{aligned}$$

la octava ecuación en Φ. Dejamos al lector la comprobación de las restantes ecuaciones.

V. Mediante las ecuaciones Φ, mostraremos que los 28 números $(1,2)$, $(1,3)$ etc. no tienen ningún divisor común. Primero observamos que se puede hacer 27 productos de tres factores tales que el primero es $\mathfrak{n}$, el segundo es uno de los números a', $2b'$, c' y el tercero es uno de los números a'', $2b''$, c''; o que el primero es $\mathfrak{n}'$, el segundo es uno de los números a, $2b$, c y el tercero uno de los números a'', $2b''$, c''; o finalmente que el primero es $\mathfrak{n}''$, el segundo uno de los números a, $2b$,

*) Observe que podríamos deducir otras 18 ecuaciones similares a Ψ reemplazando los factores a, $2b$, c por a', $2b'$, c'; a'', $2b''$, c''; pero puesto que no son necesarias para nuestros propósitos, las omitiremos.

†) Esto sigue de la ecuación 10 del artículo 235 ff. La cantidad $\sqrt{dd'}$ se hace $= Dnn' = \mathfrak{D}nn'\mathfrak{N}^2 = \mathfrak{D}\mathfrak{n}\mathfrak{n}'$.

c y el tercero uno de los números a', $2b'$, c'. Cada uno de estos 27 productos, debido a las ecuaciones Φ, será igual a uno de los 28 números $(1,2)$, $(1,3)$ etc. o la suma o diferencia de algunos de ellos (ej. $\mathfrak{n}a'a'' = (1,5)$, $2\mathfrak{n}a'b'' = (1,6)+(2,5)$, $4\mathfrak{n}b'b'' = (1,8)+(2,7)+(3,6)+(4,5)$ etc.). Por lo tanto si estos números tuvieran un divisor común, necesariamente dividiría todos estos productos. Entonces mediante el artículo 40 y el método utilizado tantas veces anteriormente, el mismo divisor también debe dividir los números $\mathfrak{n}m'm''$, $\mathfrak{n}'mm''$, $\mathfrak{n}''mm'$ y el cuadrado de este divisor debe también dividir a los cuadrados de estos números, es decir, $\frac{dm'^2m''^2}{\mathfrak{D}}$, $\frac{d'm^2m''^2}{\mathfrak{D}}$, $\frac{d'''m^2m'^2}{\mathfrak{D}}$, *Q. E. A.* , pues según I el máximo común divisor de los tres numeradores es $\mathfrak{D}$ y así estos tres cuadrados no pueden tener un divisor común.

VI. Todo esto se refiere a la transformación de la forma $\mathfrak{F}$ en $ff'f''$; y se puede deducir de la transformación de la forma F en ff' y de la forma $\mathfrak{F}$ en Ff''. De manera completamente similar se deriva la transformación de la forma $\mathfrak{F}'$ en $ff'f''$ a partir de transformaciones de la forma F' en ff'' y de la forma $\mathfrak{F}'$ en $F'f'$:

$$\mathfrak{X}' = (1)'xx'x'' + (2)'xx'y'' + (3)'xy'x'' + \text{ etc.}$$
$$\mathfrak{Y}' = (9)'xx'x'' + (10)'xx'y'' + (11)'xy'x'' + \text{ etc.}$$

(aquí los coeficientes son designados de la misma manera que en la transformación de la forma $\mathfrak{F}$ en $ff'f''$, pero se les ha puesto primos para distinguirlos). A partir de estas transformaciones deducimos, igual que antes, 28 ecuaciones análogas a las ecuaciones Φ que llamaremos Φ' y otras nueve análogas a las ecuaciones Ψ que llamaremos Ψ'. Así pues si denotamos

$$(1)'(10)' - (2)'(9)' \quad \text{por} \quad (1,2)', \qquad (1)'(11)' - (3)'(9)' \quad \text{por} \quad (1,3)', \text{ etc.}$$

las ecuaciones Φ' serán

$$(1,2)' = aa'\mathfrak{n}'', \qquad (1,3)' = aa''\mathfrak{n}', \text{ etc.}$$

y las ecuaciones Ψ' serán

$$(10)'(11)' - (9)'(12)' = a\mathfrak{n}'\mathfrak{n}''\mathfrak{A}' \text{ etc.}$$

(Para abreviar dejamos un estudio más detallado de esto al lector; el experto no necesitará realizar nuevos cálculos puesto que hay una analogía entre éste y el primer análisis). Ahora, a partir de Φ y Φ' se sigue inmediatamente que

$$(1,2) = (1,2)', \quad (1,3) = (1,3)', \quad (1,4) = (1,4)', \quad (2,3) = (2,3)', \text{ etc.}$$

Y puesto que todos los $(1,2)$, $(1,3)$, $(2,3)$, etc. no poseen un divisor común (según V), con la ayuda del lema del artículo 234 podemos determinar cuatro enteros α, β, γ, δ tales que

$$\begin{array}{lll} \alpha(1)' + \beta(9)' = (1), & \alpha(2)' + \beta(10)' = (2), & \alpha(3)' + \beta(11)' = (3) \text{ etc.} \\ \gamma(1)' + \delta(9)' = (9), & \gamma(2)' + \delta(10)' = (10), & \gamma(3)' + \delta(11)' = (11) \text{ etc.} \end{array}$$

y $\alpha\delta - \beta\gamma = 1$.

VII. Ahora, si sustituimos de las tres primeras ecuaciones de Ψ, valores para $a\mathfrak{A}$, $a\mathfrak{B}$, $a\mathfrak{C}$, y de las tres primeras ecuaciones de Ψ' los valores de $a\mathfrak{A}'$, $a\mathfrak{B}'$, $a\mathfrak{C}'$ se confirma fácilmente que:

$$\begin{aligned} a(\mathfrak{A}\alpha^2 + 2\mathfrak{B}\alpha\gamma + \mathfrak{C}\gamma^2) &= a\mathfrak{A}' \\ a(\mathfrak{A}\alpha\beta + \mathfrak{B}(\alpha\delta + \beta\gamma) + \mathfrak{C}\gamma\delta) &= a\mathfrak{B}' \\ a(\mathfrak{A}\beta^2 + 2\mathfrak{B}\beta\delta + \mathfrak{C}\delta^2) &= a\mathfrak{C}' \end{aligned}$$

y a menos que $a = 0$ se sigue que la forma $\mathfrak{F}$ se transforma en la forma $\mathfrak{F}'$ mediante la sustitución propia α, β, γ, δ. Si en lugar de las primeras tres ecuaciones de Ψ y Ψ' utilizamos las tres siguientes, obtendremos tres ecuaciones como las anteriores excepto que ahora los factores a serían reemplazados con b; y la misma conclusión es válida siempre y cuando no sea $b = 0$. Finalmente si utilizamos las últimas tres ecuaciones en Ψ y Ψ' las conclusiones son las mismas a menos que $c = 0$. Y puesto que ciertamente no todos los factores a, b, c pueden ser $= 0$ simultáneamente, la forma $\mathfrak{F}$ necesariamente se transformará en la forma $\mathfrak{F}'$ mediante la sustitución α, β, γ, δ y las formas serán propiamente equivalentes. *Q. E. D.*

241.

Si tenemos una forma como $\mathfrak{F}$ o $\mathfrak{F}'$ que resulta de la composición de una de tres formas dadas con otra la cual es la composición de las dos formas restantes, diremos que está *compuesta por estas tres formas*. Queda claro del artículo anterior que no importa el orden en el cual se componen las tres formas. Similarmente, si tenemos cualquier número de formas f, f', f'', f''', etc. (y los cocientes de sus determinantes son cuadrados) y se compone la forma f con f', la forma resultante con f'' y la resultante con f''', etc.: diremos que la última forma que se obtiene de esta operación está compuesta por *todas las formas* f, f', f'', f''', etc. Y es fácil mostrar aquí

también que el orden de composición es arbitrario; i.e. no importa en qué orden se componen estas formas, las formas resultantes serán propiamente equivalentes. Es claro también que si las formas g, g', g'', etc. son propiamente equivalentes a las formas f, f', f'', etc. respectivamente, la forma compuesta de las primeras será propiamente equivalente a la forma compuesta de las últimas.

242.

Las proposiciones anteriores se refieren a la composición de formas en toda su universalidad. Ahora pasaremos a aplicaciones más particulares que no estudiamos anteriormente para no interrumpir el orden del desarrollo. Primero retomaremos el problema del artículo 236 limitándolo según las siguientes condiciones: *primero* las formas a componer deben tener el mismo determinante, i.e. $d = d'$; *segundo*, m y m' deben ser primos relativos; *tercero*, la forma que buscamos debe ser compuesta directamente por f y f'. Entonces m^2 y m'^2 también serán primos relativos; y así el máximo común divisor de los números dm'^2 y $d'm^2$ i.e. D será $= d = d'$ y $n = n' = 1$. Puesto que podemos escogerlos libremente, haremos que las cuatro cantidades $\mathfrak{Q}$, $\mathfrak{Q}'$, $\mathfrak{Q}''$, $\mathfrak{Q}''' = -1$, 0, 0, 0 respectivamente. Esto está permitido excepto cuando a, a', $b + b'$ son todos $= 0$ simultáneamente, así que omitiremos este caso. Claramente esto no puede ocurrir excepto en formas con un determinante cuadrado positivo. Ahora, si μ es el máximo común divisor de los números a, a', $b + b'$, los números $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ pueden escogerse tales que

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b + b') = \mu$$

En cuanto a $\mathfrak{P}$, éste puede escogerse arbitrariamente. Como resultado, si sustituimos p, q, p', q' etc. por sus valores, tenemos:

$$A = \frac{aa'}{\mu^2}, \qquad B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$$

y C puede determinarse de la ecuación $AC = B^2 - D$ siempre y cuando a y a' no sean simultáneamente $= 0$.

Ahora, en esta solución el valor de A es independiente de los valores de $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ (los cuales se pueden determinar de una infinidad de maneras); pero B tendrá valores diferentes al asignar valores variados a estos números. Entonces vale

la pena investigar cómo están interconectados todos estos valores de B. Para esto observamos

I. No importa cómo se determinan $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$, todos los valores de B son congruentes según el módulo A. Supongamos que si

$$\mathfrak{P} = \mathfrak{p}, \quad \mathfrak{P}' = \mathfrak{p}', \quad \mathfrak{P}'' = \mathfrak{p}'', \quad \mathfrak{P}''' = \mathfrak{p}''' \quad \text{tenemos} \quad B = \mathfrak{B}$$

pero haciendo

$$\mathfrak{P} = \mathfrak{p} + \mathfrak{d}, \quad \mathfrak{P}' = \mathfrak{p}' + \mathfrak{d}', \quad \mathfrak{P}'' = \mathfrak{p}'' + \mathfrak{d}'', \quad \mathfrak{P}''' = \mathfrak{p}''' + \mathfrak{d}''' \quad \text{tenemos} \quad B = \mathfrak{B} + \mathfrak{D}$$

Entonces tendremos

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''' = 0, \qquad aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb'+D)\mathfrak{d}''' = \mu\mathfrak{D}$$

Multiplicando el primer miembro de la segunda ecuación por $a\mathfrak{p}' + a'\mathfrak{p}'' + (b+b')\mathfrak{p}'''$, el segundo miembro por μ, y restando del primer producto la cantidad

$$(ab'\mathfrak{p}' + a'b\mathfrak{p}'' + (bb'+D)\mathfrak{p}''')(a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''')$$

lo cual según la primera ecuación anterior es claramente $= 0$, se encontrará, después de cancelar los términos nulos que

$$aa'\{\mu\mathfrak{d} + ((b'-b)\mathfrak{p}'' + c'\mathfrak{p}''')\mathfrak{d}' - ((b-b')\mathfrak{p}' + c\mathfrak{p}''')\mathfrak{d}'' - (c'\mathfrak{p}' + c\mathfrak{p}'')\mathfrak{d}'''\} = \mu^2\mathfrak{D}$$

De donde es claro que $\mu^2\mathfrak{D}$ será divisible por aa' y $\mathfrak{D}$ por $\frac{aa'}{\mu^2}$ i.e. por A y

$$\mathfrak{B} \equiv \mathfrak{B} + \mathfrak{D} \pmod{A}$$

II. Si los valores $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, $\mathfrak{p}'''$ de $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$, $\mathfrak{P}'''$ hacen $B = \mathfrak{B}$, entonces se pueden encontrar otros valores de estos números que harán que B sea igual a cualquier número dado que sea congruente a $\mathfrak{B}$ según el módulo A, a saber $\mathfrak{B} + kA$. Primero observamos que los cuatro números μ, c, c', $b-b'$ no pueden tener un divisor común; pues si lo hubiera, sería un divisor de los seis números a, a', $b+b'$, c, c', $b-b'$ y luego de a, $2b$, c y a', $2b'$, c' y por lo tanto también de m y m' que son por hipótesis primos relativos. Así pues, se pueden encontrar cuatro enteros h, h', h'' y h''' tales que

$$h\mu + h'c + h''c' + h'''(b-b') = 1$$

Y si ponemos

$$\begin{aligned} kh &= \mathfrak{d}, & k(h''(b+b') - h'''a') &= \mu\mathfrak{d}' \\ k(h'(b+b') + h'''a) &= \mu\mathfrak{d}'', & -k(h'a' + h''a) &= \mu\mathfrak{d}''' \end{aligned}$$

es claro que $\mathfrak{d}$, $\mathfrak{d}'$, $\mathfrak{d}''$ y $\mathfrak{d}'''$ son enteros y

$$a\mathfrak{d}' + a'\mathfrak{d}'' + (b+b')\mathfrak{d}''' = 0$$
$$aa'\mathfrak{d} + ab'\mathfrak{d}' + a'b\mathfrak{d}'' + (bb' + D)\mathfrak{d}''' = \frac{aa'k}{\mu}(\mu h + ch' + c'h'' + (b-b')h''') = \mu kA$$

A partir de la primera ecuación es claro que $\mathfrak{p}+\mathfrak{d}$, $\mathfrak{p}'+\mathfrak{d}'$, $\mathfrak{p}''+\mathfrak{d}''$ y $\mathfrak{p}'''+\mathfrak{d}'''$ son también valores de $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$ y $\mathfrak{P}'''$; y de la última, que estos valores nos dan $B = \mathfrak{B} + kA$, *Q. E. D.* En este caso queda claro que B siempre puede escogerse tal que quede entre 0 y $A-1$ inclusive, para A positivo; o entre 0 y $-A-1$ para A negativo.

243.

De las ecuaciones

$$\mathfrak{P}'a + \mathfrak{P}''a' + \mathfrak{P}'''(b+b') = \mu, \qquad B = \frac{1}{\mu}(\mathfrak{P}aa' + \mathfrak{P}'ab' + \mathfrak{P}''a'b + \mathfrak{P}'''(bb' + D))$$

deducimos

$$B = b + \frac{a}{\mu}(\mathfrak{P}a' + \mathfrak{P}'(b'-b) - \mathfrak{P}'''c) = b' + \frac{a'}{\mu}(\mathfrak{P}a + \mathfrak{P}''(b-b') - \mathfrak{P}'''c')$$

y por lo tanto

$$B \equiv b \pmod{\frac{a}{\mu}} \quad \text{y} \quad B \equiv b' \pmod{\frac{a'}{\mu}}$$

Ahora, cuando $\frac{a}{\mu}$ y $\frac{a'}{\mu}$ son primos relativos, existirá entre 0 y $A-1$ (o entre 0 y $-A-1$ cuando A es negativo) sólo un número que será $\equiv b \pmod{\frac{a}{\mu}}$ y $\equiv b' \pmod{\frac{a'}{\mu}}$. Si dejamos que sea $= B$ y $\frac{B^2-D}{A} = C$ es claro que (A, B, C) estará compuesta de las formas (a, b, c) y (a', b', c'). Entonces en este caso no es necesario considerar los

números $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{P}''$ y $\mathfrak{P}'''$ para encontrar la forma compuesta*). Así pues, si se busca la forma compuesta por las formas $(10, 3, 11)$ y $(15, 2, 7)$ tendremos a, a', $b + b' = 10$, 15, 5 respectivamente; $\mu = 5$; tal que $A = 6; B \equiv 3 \pmod 2$ y $\equiv 2 \pmod 3$. Por lo tanto $B = 5$ y $(6, 5, 21)$ es la forma buscada. Pero la condición de que $\frac{a}{\mu}$ y $\frac{a'}{\mu}$ sean primos relativos es equivalente a pedir que los dos números a y a' no tengan divisor común mayor que los tres números a, a', $b + b'$ o lo que es lo mismo, que el máximo común divisor de a y a' también sea divisor del número $b + b'$. Se notan los siguientes casos particulares.

1) Suponga que tenemos dos formas (a, b, c) y (a', b', c') con el mismo determinante D y relacionadas tales que el máximo común divisor de los números a, $2b$, c es primo relativo al máximo común divisor de a', $2b'$, c' y que a y a' son primos relativos: entonces la forma (A, B, C), que es la composición de estas dos, se encuentra haciendo $A = aa'$, $B \equiv b \pmod a$ y $\equiv b' \pmod{a'}$, $C = \frac{B^2 - D}{A}$. Este caso siempre ocurrirá cuando una de las dos formas a ser compuestas es la forma principal; esto es $a = 1$, $b = 0$, $c = -D$. Luego $A = a'$, B se puede tomar $= b'$ y tendremos $C = c'$; así pues *cualquier forma está compuesta de sí misma y de la forma principal del mismo determinante.*

2) Si queremos componer dos formas *opuestas* propiamente primitivas, esto es (a, b, c) y $(a, -b, c)$, tendremos $\mu = a$. Es fácil ver que la forma principal $(1, 0, -D)$ está compuesta por estas dos.

3) Suponga que tenemos un número arbitrario de formas propiamente primitivas (a, b, c), (a', b', c'), (a'', b'', c''), etc. con el mismo determinante y con los primeros términos a, a', a'', etc. primos relativos entre sí. Entonces se puede encontrar la forma (A, B, C) compuesta por todas ellas fijando A igual al producto de todos los a, a', a'', etc.; tomando B congruente a b, b', b'', etc. respecto a los módulos a, a', a'', etc. respectivamente; y haciendo $C = \frac{B^2 - D}{A}$. Obviamente la forma $(aa', B, \frac{B^2 - D}{aa'})$ estará compuesta por las dos formas (a, b, c) y (a', b', c'); la forma $(aa'a'', B, \frac{B^2 - D}{aa'a''})$ estará compuesta por las formas $(aa', B, \frac{B^2 - D}{aa'})$ y (a'', b'', c'') etc. En cambio

4) Suponga que tenemos una forma (A, B, C) propiamente primitiva de determinante D. Si se resuelve el término A en un número cualquiera de factores

*) Podemos lograrlo siempre utilizando las congruencias

$$\frac{aB}{\mu} \equiv \frac{ab'}{\mu}, \quad \frac{a'B}{\mu} \equiv \frac{a'b}{\mu}, \quad \frac{(b + b')B}{\mu} \equiv \frac{(bb' + D)}{\mu} \pmod A.$$

primos relativos a, a', a'', etc.; si se toman los números b, b', b'', etc. todos iguales a B o por lo menos congruentes a B según los módulos a, a', a'', etc. respectivamente; y si c, c', c'', etc. son tales que $ac = b^2 - D$, $a'c' = b'^2 - D$, $a''c'' = b''^2 - D$, etc.: entonces la forma (A, B, C) estará compuesta por las formas (a, b, c), (a', b', c'), (a'', b'', c''), etc., o diremos que *se puede descomponer en estas formas*. Es fácil demostrar que esta proposición es también válida cuando la forma (A, B, C) es impropiamente primitiva u obtenida a partir de una forma de tal tipo. Así, de esta manera, cualquier forma puede resolverse en otras con el mismo determinante, en las cuales los primeros términos son números primos o potencias de números primos. Tal descomposición en muchos casos puede ser muy útil si queremos componer una forma a partir de varias formas dadas. Así pues, por ejemplo, si queremos una forma compuesta de las formas $(3, 1, 134)$, $(10, 3, 41)$ y $(15, 2, 27)$, descomponemos la segunda en $(2, 1, 201)$ y $(5, -2, 81)$, la tercera en $(3, -1, 134)$ y $(5, 2, 81)$. Es claro que la forma compuesta por las cinco formas $(3, 1, 134)$, $(2, 1, 201)$, $(5, -2, 81)$, $(3, -1, 134)$ y $(5, 2, 81)$ independientemente del orden en el cual se toman, también será una composición de las tres formas originales. Ahora, la composición de la primera con la cuarta da la forma principal $(1, 0, 401)$; y lo mismo resulta de la composición de la tercera con la quinta; así de la composición de las cinco obtenemos la forma $(2, 1, 201)$.

5) Debido a su utilidad es conveniente describir más detalladamente este método. De la observación anterior es claro que siempre y cuando las formas dadas son propiamente primitivas con el mismo determinante, el problema se puede reducir a la composición de formas cuyos términos iniciales son potencias de números primos (puesto que un número primo se puede considerar como su propia primera potencia). Por esta razón es apropiado considerar el caso especial en el cual se componen dos formas propiamente primitivas (a, b, c) y (a', b', c') siendo a y a' potencias del *mismo* número primo. Por lo tanto, sean $a = h^\chi$, $a' = h^\lambda$, donde h es un número primo y vamos a suponer que χ no es menor que λ (lo cual es legítimo). Ahora h^λ será el máximo común divisor de los números a, a'. Si además es divisor de $b + b'$ tendremos el caso que consideramos al inicio del artículo y la forma (A, B, C) será la forma compuesta si $A = h^{\chi-\lambda}$, $B \equiv b \pmod{h^{\chi-\lambda}}$ y $\equiv b' \pmod{1}$. Esta última condición obviamente puede omitirse. Finalmente $C = \frac{B^2 - D}{A}$. Si h^λ no divide a $b + b'$, el máximo común divisor de estos números será necesariamente una potencia de h, digamos h^ν con $\nu < \lambda$ (donde $\nu = 0$ si h^λ y $b + b'$ son primos entre sí). Si $\mathfrak{P}'$, $\mathfrak{P}''$ y $\mathfrak{P}'''$ se determinan de modo que

$$\mathfrak{P}' h^\chi + \mathfrak{P}'' h^\lambda + \mathfrak{P}'''(b + b') = h^\nu$$

con $\mathfrak{P}$ arbitrario, la forma (A, B, C) será compuesta de las formas dadas si se escoge

$$A = h^{\chi+\lambda-2\nu}, \qquad B = b + h^{\chi-\nu}(\mathfrak{P}h^{\lambda} - \mathfrak{P}'(b - b') - \mathfrak{P}'''c), \qquad C = \frac{B^2 - D}{A}$$

Pero es fácil ver que en este caso también $\mathfrak{P}'$ puede escogerse arbitrariamente; entonces poniendo $\mathfrak{P} = \mathfrak{P}' = 0$ resulta

$$B = b - \mathfrak{P}'''ch^{\chi-\nu}$$

o más generalmente

$$B = kA + b - \mathfrak{P}'''ch^{\chi-\nu}$$

donde k es un número arbitrario (artículo anterior). Sólo $\mathfrak{P}'''$ entra en esta fórmula muy sencilla, y es el valor de la expresión $\frac{h^{\nu}}{b+b'} \pmod{h^{\lambda}}$*). Si, por ejemplo, se busca la forma compuesta de $(16, 3, 19)$ y $(8, 1, 37)$, resulta $h = 2$, $\chi = 4$, $\lambda = 3$, $\nu = 2$. Por esto $A = 8$ y $\mathfrak{P}'''$ es un valor de la expresión $\frac{4}{4} \pmod 8$, digamos 1, de donde $B = 8k - 73$, y poniendo $k = 9$, $B = -1$ y $C = 37$, la forma buscada es $(8, -1, 37)$.

Entonces, si se proponen varias formas cuyos términos iniciales son todos potencias de números primos, hay que examinar si algunos de estos términos son potencias del *mismo* número primo y, en este caso, las formas se componen de acuerdo con las reglas que acabamos de dar. Así se obtienen formas cuyos primeros términos son potencias de números primos diferentes. La forma compuesta de éstas puede encontrarse por la tercera observación. Por ejemplo, cuando se proponen las formas $(3, 1, 47)$, $(4, 0, 35)$, $(5, 0, 28)$, $(16, 2, 9)$, $(9, 7, 21)$ y $(16, 6, 11)$, de la primera y la quinta resulta $(27, 7, 7)$; de la segunda y la cuarta $(16, -6, 11)$; y de ésta y la sexta $(1, 0, 140)$, que puede omitirse. Se quedan $(5, 0, 28)$ y $(27, 7, 7)$ que producen $(135, -20, 4)$, que se reemplaza con la forma propiamente equivalente $(4, 0, 35)$. Esta es la forma que resulta de la composición de las seis formas propuestas.

Similarmente pueden desarrollarse más artificios útiles en la práctica, pero nos obligamos a suprimir esta dirección para pasar a asuntos más difíciles.

244.

Si el número a puede ser representado por alguna forma f, el número a' por la forma f', y si la forma F es transformable en ff': no es difícil ver que el producto

*) o sea, de la expresión $\frac{1}{\frac{b+b'}{h^{\nu}}} \pmod{h^{\lambda-\nu}}$, de donde $B \equiv b - \frac{ch^{\chi-\lambda}}{\frac{b+b'}{h^{\nu}}} \equiv \frac{(D+bb')/h^{\nu}}{(b+b')/h^{\nu}} \pmod A$.

aa' será representable por la forma F. Se sigue inmediatamente que cuando los determinantes de estas formas sean negativos, la forma F será positiva si ambas f y f' son positivas o ambas negativas; al contrario F será negativa si una de las formas f y f' es positiva y la otra es negativa. Detengámonos particularmente en el caso que hemos considerado en el artículo previo, donde F está compuesta por f y f' y f, f' y F tienen el mismo determinante D. Además, supongamos que las representaciones de los números a y a' por las formas f y f' se hacen por medio de valores relativamente primos de los incógnitas. Supondremos también que la primera pertenece al valor b de la expresión $\sqrt{D} \pmod{a}$, la última al valor b' de la expresión $\sqrt{D} \pmod{a'}$ y que $b^2 - D = ac$, $b'^2 - D = a'c'$. Luego, por el artículo 168, las formas (a, b, c) y (a', b', c') serán propiamente equivalentes a las formas f y f', de modo que F estará compuesta por esas dos formas. Pero la forma (A, B, C) estará compuesta por las mismas formas si el máximo común divisor de los números a, a', $b + b'$ es μ, y si se fijan $A = \frac{aa'}{\mu^2}$, $B \equiv b, \equiv b'$ según los módulos $\frac{a}{\mu}$, $\frac{a'}{\mu}$ respectivamente, $AC = B^2 - D$; y esta forma será propiamente equivalente a la forma F. Ahora bien, el número aa' está representado por la forma $Ax^2 + 2Bxy + Cy^2$, haciendo $x = \mu$, $y = 0$ cuyo máximo común divisor es μ; de modo que aa' puede ser también representado por la forma F de manera que los valores de las incógnitas tengan a μ como su máximo común divisor (art. 166). Siempre y cuando μ sea 1, aa' puede ser representado por la forma F asignando valores primos entre sí a las incógnitas, y esta representación pertenecerá al valor B de la expresión $\sqrt{D} \pmod{aa'}$, la cual es congruente con b y b' según los módulos a y a' respectivamente. La condición $\mu = 1$ siempre tiene lugar cuando a y a' son primos entre sí; o más generalmente cuando el máximo común divisor de a y a' es primo a $b + b'$.

Composición de órdenes.

245.

TEOREMA. *Si la forma f pertenece al mismo orden que g, y f' es del mismo orden que g', entonces la forma F compuesta por f y f' tendrá el mismo determinante y será del mismo orden que la forma G compuesta por g y g'.*

Demostración. Sean las formas f, f' y F que son $= (a, b, c)$, (a', b', c') y (A, B, C), respectivamente, y sean sus determinantes $= d$, d' y D. Seguidamente sea m el máximo común divisor de los números a, $2b$ y c y sea $\mathfrak{m}$ el máximo común divisor de los números a, b y c; y que m', $\mathfrak{m}'$ con respecto a la forma f' y M, $\mathfrak{M}$ con respecto a la forma F tengan similares significados. Entonces el orden de la forma

f será determinado por los números d, m y $\mathfrak{m}$, de donde estos números también serán válidos para la forma g; por la misma razón los números d', m' y $\mathfrak{m}'$ jugarán el mismo rol para la forma g' como para la forma f'. Ahora bien, por el artículo 235, los números D, M y $\mathfrak{M}$ están determinados por d, d', m, m', $\mathfrak{m}$ y $\mathfrak{m}'$; esto es, D será el máximo común divisor de $dm'^2, d'm^2$; $M = mm'$; $\mathfrak{M} = \mathfrak{m}\mathfrak{m}'$ (si $m = \mathfrak{m}$ y $m' = \mathfrak{m}'$) ó $= 2\mathfrak{m}\mathfrak{m}'$ (si $m = 2\mathfrak{m}$ ó $m' = 2\mathfrak{m}'$). Dado que estas propiedades de D, M y $\mathfrak{M}$ se siguen del hecho de que F está compuesta por f y f', es fácil ver que D, M y $\mathfrak{M}$ juegan la misma función para la forma G, así que G es del mismo orden que F. *Q. E. D.*

Por esta razón diremos que el orden de la forma F está compuesto de los órdenes de las formas f y f'. De este modo, p.ej., si tenemos dos órdenes propiamente primitivos, su composición será propiamente primitiva; si uno es propiamente primitivo y el otro impropiamente primitivo, la composición será impropiamente primitiva. Se debe entender de una manera similar si se dice que un orden está compuesto de varios otros órdenes.

Composición de géneros.

246.

PROBLEMA. *Propuestas dos formas primitivas cualesquiera f y f' y la forma F compuesta de estas dos: determinar el género al cual pertenece F a partir de los géneros a los cuales pertenecen f y f'.*

Solución. I. Consideremos primero el caso donde al menos una de las formas f o f' (p.ej. la primera) es propiamente primitiva, y designemos los determinantes de las formas f, f' y F por d, d' y D. D será el máximo común divisor de los números dm'^2 y d', donde m' es 1 ó 2 según la forma f' sea propia o impropiamente primitiva. En el primer caso F pertenecerá a un orden propiamente primitivo, en el segundo a un orden impropiamente primitivo. Ahora bien, el género de la forma F estará definido por sus caracteres particulares, esto es con respecto a los divisores impares primos individuales de D y también para algunos casos con respecto a los números 4 y 8. Será conveniente considerar estos casos separadamente.

1. Si p es un divisor impar primo de D, necesariamente dividirá a d y a d', y así también entre los caracteres de las formas f y f' se encuentran las relaciones de F con p. Ahora bien, si el número a puede ser representado por f, y el número a' por f', el producto aa' puede ser representado por F. Así que si los residuos cuadráticos de p (no divisibles por p) pueden ser representados tanto por f como por f', ellos

pueden ser también representados por F; i.e. si ambos f y f' tienen el carácter Rp, la forma F tendrá el mismo carácter. Por una razón similar F tendrá el carácter Rp si ambos f y f' tienen el carácter Np; contrariamente F tendrá al carácter Np si una de las formas f o f' tiene el carácter Rp y la otra tiene el carácter Np.

2. Si una relación con el número 4 entra dentro del carácter total de la forma F, tal relación también debe entrar dentro de los caracteres de las formas f y f'. En efecto, esto sólo puede pasar cuando D es $\equiv 0$ ó $\equiv 3 \pmod 4$. Cuando D es divisible por 4, dm'^2 y d' son también divisibles por 4, y es inmediatamente claro que f' no puede ser impropiamante primitiva y así $m' = 1$. Luego tanto d como d' son divisibles por 4 y una relación con 4 entrará dentro del carácter de cada cual. Cuando $D \equiv 3 \pmod 4$, D dividirá a d y a d', los cocientes serán cuadrados y así d y d' serán necesariamente $\equiv 0$ ó $\equiv 3 \pmod 4$ y una relación con el número 4 estará incluida entre los caracteres de f y f'. De este modo, así como en (1), se seguirá que el carácter de la forma F será 1, 4 si ambos f y f' tienen el carácter 1, 4 ó 3, 4; contrariamente el carácter de la forma F será 3, 4 si una de las formas f o f' tiene el carácter 1, 4 y la otra 3, 4.

3. Cuando D es divisible por 8, d' lo será también; de donde f' seguramente será propiamente primitivo, $m' = 1$ y d también será divisible por 8. Y así uno de los caracteres 1, 8; 3, 8; 5, 8; 7, 8 aparecerá entre los caracteres de la forma F sólo si tal relación con 8 aparece también en el carácter de ambas formas f y f'. De la misma manera como antes, es fácil ver que 1, 8 será un carácter de la forma F si f y f' tienen el mismo carácter con respecto a 8; que 3, 8 será un carácter de la forma F si una de las formas f o f' tiene el carácter 1, 8, la otra 3, 8; ó una de ellas tiene el carácter 5, 8 y la otra 7, 8; F tendrá el carácter 5, 8 si f y f' tienen 1, 8 y 5, 8 ó 3, 8 y 7, 8; y F tendrá el carácter 7, 8 si f y f' tienen ya sea 1, 8 y 7, 8 ó 3, 8 y 5, 8 como caracteres.

4. Cuando $D \equiv 2 \pmod 8$, d' será $\equiv 0$ ó $\equiv 2 \pmod 8$, así que $m' = 1$ y d será también $\equiv 0$ ó $\equiv 2 \pmod 8$; pero dado que D es el *máximo* común divisor de d y d', ellos no pueden ser ambos divisibles por 8. Entonces en este caso el carácter de la forma F sólo puede ser 1 *y* 7, 8 ó 3 *y* 5, 8 cuando ambas formas f y f' tienen uno de estos caracteres y el otro tiene uno de los siguientes: 1, 8; 3, 8; 5, 8; 7, 8. La siguiente tabla determinará el carácter de la forma F. El carácter en el margen pertenece a una de las formas f o f', y el carácter en la cabeza de las columnas pertenece a la otra.

	1 *y* 7, 8 o 1,8 o 7, 8	3 *y* 5, 8 o 3, 8 o 5, 8
1 *y* 7, 8	1 *y* 7, 8	3 *y* 5, 8
3 *y* 5, 8	3 *y* 5, 8	1 *y* 7, 8

5. De la misma manera, puede ser probado que F no puede tener el carácter 1 *y* 3, 8 ó 5 *y* 7, 8 a no ser que al menos una de las formas f o f' tenga a uno de estos caracteres. La otra puede tener uno de ellos también o uno de éstos: 1, 8; 3, 8; 5, 8; 7, 8. El carácter de la forma F está determinado por la siguiente tabla. Los caracteres de las formas f y f' de nuevo aparecen en el margen y en la cabeza de las columnas.

	1 *y* 3, 8 o 1,8 o 3, 8	5 *y* 7, 8 o 5, 8 o 7, 8
1 *y* 3, 8	1 *y* 3, 8	5 *y* 7, 8
5 *y* 7, 8	5 *y* 7, 8	1 *y* 3, 8

II. Si cada una de las formas f y f' es impropiamente primitiva, D será el máximo común divisor de los números $4d$, $4d'$ o sea $\frac{1}{4}D$ el máximo común divisor de los números d, d'. Se sigue que d, d' y $\frac{1}{4}D$ serán todos $\equiv 1 \pmod 4$. Poniendo $F = (A, B, C)$, el máximo común divisor de los números A, B, C será $= 2$, y el máximo común divisor de los números A, $2B$, C será 4. Luego F será una forma derivada de la forma impropiamente primitiva $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$, cuyo determinante será $\frac{1}{4}D$, y su género determinará el género de la forma F. Pero, dado que es impropiamente primitiva, su carácter no implicará relaciones con 4 u 8, sino sólo con los divisores impares primos individuales de $\frac{1}{4}D$. Ahora todos estos divisores manifiestamente dividen también a d y a d', y si los dos factores de un producto son representables uno por f, el otro por f', entonces la mitad del producto es representable por la forma $(\frac{1}{2}A, \frac{1}{2}B, \frac{1}{2}C)$. Se sigue que el carácter de esta forma con respecto a cualquier número impar primo p que divida a $\frac{1}{4}D$ será Rp cuando $2Rp$ y las formas f, f' tengan el mismo carácter con respecto a p y cuando $2Np$ y los caracteres de f y f' con respecto a p son opuestos. Contrariamente el carácter de la forma será Np cuando f y f' tengan iguales caracteres con respecto a p y $2Np$, y cuando f y f' tengan caracteres opuestos y se tiene $2Rp$.

247.

De la solución del problema precedente, es manifiesto que si g es una forma primitiva del mismo orden y género que f, y g' es una forma primitiva del mismo orden y género que f': entonces la forma compuesta por g y g' será del mismo género que la forma compuesta por f y f'. Así se ve lo que significa un *género compuesto* por dos (o incluso varios) géneros. Además, si f y f' tienen el mismo determinante, f es una forma del género principal, y F está compuesta por f y f': entonces F será del mismo género que f'; de ahí que el género principal puede siempre ser omitido en la composición de otros géneros del mismo determinante. Es así como, siendo otras cosas iguales, si f no está en el género principal y f' es una forma primitiva, F ciertamente estará en un género que no es f'. Finalmente, si f y f' son formas propiamente primitivas del mismo género, F estará en el género principal; si, de hecho f y f' son ambas propiamente primitivas con el mismo determinante pero en distintos géneros, F no puede pertenecer al género principal. Y si una forma propiamente primitiva se compone *consigo misma*, la forma resultante, la cual también será propiamente primitiva con el mismo determinante, necesariamente pertenecerá al género principal.

248.

Problema. *Dadas dos formas cualesquiera, f y f' de las cuales F está compuesta: determinar el género de la forma F a partir de aquéllos de las formas f y f'.*

Solución. Sean $f = (a, b, c)$, $f' = (a', b', c')$ y $F = (A, B, C)$; de seguido, desígnase por $\mathfrak{m}$ el máximo común divisor de los números a, b, c y por $\mathfrak{m}'$ el maximo común divisor de los números a', b', c', de modo que las formas f y f' sean derivadas de las formas primitivas $(\frac{a}{\mathfrak{m}}, \frac{b}{\mathfrak{m}}, \frac{c}{\mathfrak{m}})$ y $(\frac{a'}{\mathfrak{m}'}, \frac{b'}{\mathfrak{m}'}, \frac{c'}{\mathfrak{m}'})$, las que designaremos por $\mathfrak{f}$ y $\mathfrak{f}'$ respectivamente. Ahora si al menos una de las formas $\mathfrak{f}$ o $\mathfrak{f}'$ es propiamente primitiva, el máximo común divisor de los números A, B, C será $\mathfrak{m}\mathfrak{m}'$, y por ende F será derivado de la forma primitiva $(\frac{A}{\mathfrak{m}\mathfrak{m}'}, \frac{B}{\mathfrak{m}\mathfrak{m}'}, \frac{C}{\mathfrak{m}\mathfrak{m}'}) \ldots \mathfrak{F}$ y es claro que el género de la forma F dependerá del de la forma $\mathfrak{F}$. Es fácil ver que si $\mathfrak{F}$ es transformado en $\mathfrak{f}\mathfrak{f}'$ por la misma sustitución que transforma a F en ff' y de tal modo que $\mathfrak{F}$ está compuesto por $\mathfrak{f}$ y $\mathfrak{f}'$, su género puede ser determinado por el problema del artículo 246. Pero si ambas $\mathfrak{f}$ y $\mathfrak{f}'$ son impropiamente primitivas, el máximo común divisor de los números A, B, C será $2\mathfrak{m}\mathfrak{m}'$, y la forma $\mathfrak{F}$, que está todavía compuesta por $\mathfrak{f}$ y $\mathfrak{f}'$, será manifiestamente derivada de la forma propiamente primitiva $(\frac{A}{2\mathfrak{m}\mathfrak{m}'}, \frac{B}{2\mathfrak{m}\mathfrak{m}'}, \frac{C}{2\mathfrak{m}\mathfrak{m}'})$. El género de esta

forma puede ser determinado por el artículo 246 y dado que F está derivado de la misma manera, su género será conocido asímismo.

A partir de esta solución es manifiesto que el teorema en el artículo precedente, que ha sido restringido a las formas primitivas, es válido para cualquier forma, a saber: *si f' y g' son de los mismos géneros respectivamente que f y g, la forma compuesta por f' y g' será del mismo género que la forma compuesta por f y g.*

Composición de Clases.

249.

TEOREMA. *Si las formas f y f' son de los mismos órdenes, géneros y clases que g y g' respectivamente, entonces la forma compuesta por f y f' será de la misma clase que la forma compuesta por g y g'.*

De este teorema (cuya verdad se sigue inmediatamente del artículo 239) es evidente lo que queremos decir cuando hablamos de una *clase compuesta por dos (o más) clases dadas.*

Si cualquier clase K está compuesta con una clase principal, el resultado será la clase K misma; esto es, en composición con otras clases del mismo determinante una clase principal puede ser ignorada. De la composición de dos clases propiamente primitivas opuestas siempre obtendremos una clase principal del mismo determinante (véase artículo 243). Dado que por este motivo cualquier clase ambigua es opuesta a sí misma, siempre obtendremos una clase principal del mismo determinante si componemos cualquier clase propiamente primitiva ambigua consigo misma.

El recíproco de la última proposición también vale; esto es *si de la composición de una clase K propiamente primitiva consigo misma proviene una clase principal H con el mismo determinante, K necesariamente será una clase ambigua.* Puesto que si K' es una clase opuesta a K, la misma clase surgirá de la composición de H y K' como de las tres clases K, K y K'; a partir de las últimas proviene K (dado que K y K' producen a H, y H y K producen a K). De las primeras obtenemos K'; de ahí que K y K' coinciden y la clase es ambigua.

Ahora se nota la proposición siguiente: *Si las clases K y L son opuestas a las clases K' y L' respectivamente, la clase compuesta por K y L será opuesta a la clase compuesta por K' y L'.* Sean f, g, f' y g' las formas de las clases K, L, K' y L' respectivamente, y sea F compuesta por f y g, y F' compuesta por f' y g'. Dado que f' es impropiamente equivalente a f, y g' impropiamente equivalente a g, mientras que F está compuesto por ambas f y g directamente: F estará también compuesta

por f' y g' pero con cada una de ellas indirectamente. De este modo cualquier forma que es impropiamente equivalente a F estará compuesta por f' y g' directamente y así será propiamente equivalente a F' (art. 238, 239). De ahí que F y F' serán impropiamente equivalentes y las clases a las que pertenecen son opuestas.

Sigue de esto que, si se compone una clase ambigua K con una clase ambigua L, siempre se produce una clase ambigua. En efecto, ella será opuesta a la clase que es compuesta de las clases opuestas a K y L; a saber, a sí misma, ya que estas clases son opuestas a sí mismas.

Finalmente observamos que si se proponen dos clases cualesquiera K y L del mismo determinante y la primera es propiamente primitiva, siempre podemos encontrar una clase M con el mismo determinante tal que L esté compuesta por M y K. Manifiestamente esto puede hacerse tomando por M la clase que está compuesta por L y la clase opuesta a K; es fácil ver que esta clase es la única que disfruta de esta propiedad; es decir, si componemos diferentes clases del mismo determinante con la misma clase propiamente primitiva, se producen distintas clases.

Es conveniente denotar la composición de clases por el signo de adición, $+$, y la identidad de clases por el signo de igualdad. Usando estos signos la proposición recién considerada puede ser enunciada como sigue: Si la clase K' es opuesta a K, $K+K'$ será una clase principal del mismo determinante, de modo que $K+K'+L = L$; si se toma $K' + L = M$, tenemos $K + M = L$, como se desea. Ahora, si además de M tenemos otra clase M' con la misma propiedad, esto es $K + M' = L$, tendremos $K+K'+M' = L+K' = M$ y así $M' = M$. Si muchas clases idénticas son compuestas, esto puede indicarse (como en la multiplicación) prefijando su número, así que $2K$ significa lo mismo que $K + K$, $3K$ lo mismo que $K + K + K$, etc. Podríamos también transferir los mismos signos a formas de tal modo que $(a, b, c) + (a', b', c')$ indicaría a la forma compuesta por (a, b, c) y (a', b', c'); pero para evitar ambigüedad preferimos no usar esta abreviación, especialmente puesto que ya habíamos asignado un significado especial al símbolo $\sqrt{M}(a, b, c)$. Diremos que la clase $2K$ surge de la *duplicación* de la clase K, la clase $3K$ de la *triplicación*, etc.

250.

Si D es un número divisible por m^2 (suponemos a m positivo), habrá un orden de formas de determinante D derivado del orden propiamente primitivo del determinante $\frac{D}{m^2}$ (cuando D es negativo habrá *dos* de ellos, uno positivo y uno negativo); manifiestamente la forma $(m, 0, -\frac{D}{m})$ pertenecerá a aquel orden (el

positivo) y puede ser correctamente considerada la *forma más simple* en el orden (justo como $(-m,\, 0,\, \frac{D}{m})$ será la más simple en el orden negativo cuando D es negativo). Si además tenemos $\frac{D}{m^2} \equiv 1 \pmod 4$, habrá también un orden de formas de determinante D derivado del determinante impropiamente primitivo $\frac{D}{m^2}$. La forma $(2m,\, m,\, \frac{m^2-D}{2m})$ pertenecerá a éste y será la más simple en el orden. (Cuando D es negativo, habrá de nuevo dos órdenes y en el orden negativo $(-2m,\, -m,\, \frac{D-m^2}{2m})$ será la forma más simple.) Así, e.g., si aplicamos esto al caso donde $m = 1$, el siguiente será el más simple entre los cuatro órdenes de formas con determinante 45; $(1,\, 0,\, -45)$, $(2,\, 1,\, -22)$, $(3,\, 0,\, -15)$, $(6,\, 3,\, -6)$.

Todas estas consideraciones dan lugar a lo siguiente.

PROBLEMA. *Dada cualquier forma F del orden O, encontrar una forma propiamente primitiva (positiva) del mismo determinante que produzca F cuando está compuesta con la forma más simple en O.*

Solución. Sea la forma $F = (ma,\, mb,\, mc)$ derivada de la forma primitiva $f = (a,\, b,\, c)$ de determinante d y supondremos *primero* que f es propiamente primitiva. Observamos que si a y $2dm$ no son primos entre sí, ciertamente hay otras formas propiamente equivalentes a $(a,\, b,\, c)$ cuyos primeros términos tienen esta propiedad. Debido al artículo 228, hay números primos a $2dm$ representables por esta forma. Sea tal número $a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$ y supondremos (es legítimo hacerlo) que α y γ son primos entre sí. Ahora si escogemos β y δ tales que $\alpha\delta - \beta\gamma = 1$, f será transformada por la sustitución $\alpha,\, \beta,\, \gamma,\, \delta$ en la forma $(a',\, b',\, c')$ que es propiamente equivalente a ella y tiene la propiedad prescrita. Ahora, dado que F y $(a'm,\, b'm, c'm)$ son propiamente equivalentes es suficiente considerar el caso donde a y $2dm$ son relativamente primos. Ahora $(a,\, bm,\, cm^2)$ será una forma propiamente primitiva del mismo determinante que F (pues si $a, 2bm, cm^2$ tuvieran un divisor común, también significaría que él divide a $2dm = 2b^2m - 2acm$). Es fácil confirmar que F será transformada en el producto de las formas $(m,\, 0,\, -dm)$ y $(a,\, bm,\, cm^2)$ por la sustitución $1,\, 0,\, -b,\, -cm;\ 0,\, m,\, a,\, bm$. Note que, a no ser que F sea una forma negativa, $(m,\, 0,\, -dm)$ será la forma más simple del orden O. Usando el criterio de la cuarta observación en el artículo 235, se concluye que F está compuesta por $(m,\, 0,\, -dm)$ y $(a,\, bm,\, cm^2)$. Cuando de todos modos F es una forma negativa, será transformada por la sustitución $1,\, 0,\, b,\, -cm;\ 0,\, -m,\, -a,\, bm$ en el producto de $(-m,\, 0,\, dm)$, la forma más simple del mismo orden, y la forma positiva $(-a,\, bm,\, -cm^2)$ y así estará compuesta por estas dos.

Segundo, si f es una forma impropiamente primitiva, se puede suponer que

$\frac{1}{2}a$ y $2dm$ son primos entre sí; pues si esta propiedad no es cierta ya, de la forma f se puede encontrar una forma propiamente equivalente a f que tenga la propiedad. De esto se sigue fácilmente que $(\frac{1}{2}a,\ bm,\ 2cm^2)$ es una forma propiamente primitiva del mismo determinante que F; y es igualmente fácil confirmar que F será transformada en el producto de las formas

$$(\pm 2m,\ \pm m,\ \pm\frac{1}{2}(m - dm)) \quad \text{y} \quad (\pm\frac{1}{2}a,\ bm,\ \pm 2cm^2)$$

por la sustitución

$$1,\ 0,\ \frac{1}{2}(1 \mp b),\ -cm \quad ; \quad 0,\ \pm 2m,\ \pm\frac{1}{2}a,\ (b+1)m$$

donde los signos inferiores deben ser tomados cuando F es una forma negativa y los signos superiores en caso contrario. Concluimos que F está compuesta por estas dos formas y la primera es la más simple de orden O, la última es una forma propiamente primitiva (positiva).

251.

PROBLEMA. *Dadas dos formas F y f del mismo determinante D y pertenecientes al mismo orden O: encontrar una forma propiamente primitiva de determinante D que produzca a F cuando ésta esté compuesta con f.*

Solución. Sea φ la forma más simple de orden O; $\mathfrak{F}$ y $\mathfrak{f}$ formas propiamente primitivas de determinante D que producen a F y f respectivamente cuando están compuestas con φ; y sea f' la forma propiamente primitiva que produce a $\mathfrak{F}$ cuando está compuesta con $\mathfrak{f}$. Entonces la forma F estará compuesta de las tres formas φ, $\mathfrak{f}$ y f' ó de las dos formas f y f'. *Q. E. I.*

De ahí que toda clase de un orden dado puede ser considerada como compuesta por cualquier clase dada del mismo orden y otra clase propiamente primitiva del mismo determinante.

Para un determinante dado existe el mismo número de clases en cada género del mismo orden.

252.

TEOREMA. *Para un determinante dado existe el mismo número de clases en cada género del mismo orden.*

Demostración. Suponga que los géneros G y H pertenecen al mismo orden, que G está compuesta por n clases K, K', K'', $\ldots K^{n-1}$ y que L es cualquier clase del género H. Por el artículo precedente se encuentra una clase propiamente primitiva M del mismo determinante cuya composición con K produce a L, y se designan por L', L'', $\ldots L^{n-1}$ a las clases que surgen de la composición de la clase M con K', K'', $\ldots K^{n-1}$ respectivamente. Entonces a partir de la última observación del artículo 249, se sigue que todas las clases L, L', L'', $\ldots L^{n-1}$ son distintas, y por el artículo 248 que todas ellas pertenecen al mismo género H. Finalmente es fácil ver que H no puede contener ninguna otra clase más que éstas, dado que cada clase del género H puede ser considerada como compuesta por M y otra clase del mismo determinante, y éste necesariamente debe ser del género G. De ahí que H, como G, contendrá n clases distintas. *Q. E. D.*

Se compara el número de clases contenidas
en géneros individuales de órdenes distintos.

253.

El teorema precedente supone la identidad del orden y no puede ser extendido a distintos órdenes. Así por ejemplo para el determinante -171 hay 20 clases positivas que son reducidas a cuatro órdenes: en el orden propiamente primitivo hay dos géneros y cada cual contiene seis clases; en el orden impropiamente primitivo dos géneros tienen cuatro clases, dos en cada cual; en el orden derivado a partir del orden propiamente primitivo de determinante -19 hay sólo un género que contiene tres clases; finalmente, el orden derivado del orden impropiamente primitivo de determinante -19 tiene un género con una clase. Lo mismo es cierto para las clases negativas. Es útil, por ende, inquirir sobre el principio general que gobierna la relación entre el número de clases en órdenes diferentes. Supóngase que K y L son dos clases del mismo orden (positivo) O de determinante D, y M es una clase propiamente primitiva del mismo determinante que produce a L cuando está compuesta con K. Por el artículo 251 tal clase siempre puede ser encontrada. Ahora bien, en algunos casos ocurre que M es la *única* clase propiamente primitiva con esta propiedad; en otros casos puede existir varias clases propiamente primitivas con esta propiedad. Supongamos en general que hay r clases propiamente primitivas de este tipo M, M', M'', $\ldots M^{r-1}$ y que cada uno de ellas produce a L cuando está compuesta con K. Designaremos este conjunto por la letra W. Ahora sea L' otra clase del orden O (distinta de la clase L), y sea N' una clase propiamente primitiva

de determinante D la cual resulta en L' cuando está compuesta con L. Usaremos W' para designar el conjunto de las clases $N'+M$, $N'+M'$, $N'+M''$, $\ldots N'+M^{r-1}$ (todas éstas serán propiamente primitivas y distintas una de la otra). Es fácil ver que K producirá a L' si ésta está compuesta con cualquier otra clase de W', y por eso concluimos que W y W' no tienen clases en común; y cada clase propiamente primitiva que produzca a L' cuando esté compuesta con K está contenida en W'. De la misma manera, si L'' es otra clase de orden O distinta de L y L', entonces habrá r formas propiamente primitivas todas distintas una de la otra y de las formas en W y W', cada una de ellas producirá a L'' cuando esté compuesta con K. Lo mismo es cierto para todas las otras clases del orden O. Ahora bien, dado que cualquier clase propiamente primitiva (positiva) de determinante D produce una clase de orden O cuando está compuesta con K, es claro que si el número de todas las clases de orden O es n, el número de todas las clases propiamente primitivas (positivas) del mismo determinante será rn. De este modo tenemos una regla general: Si denotamos por K y L dos clases cualesquiera de orden O y por r el número de clases propiamente primitivas distintas pero del mismo determinante, cada una de las cuales produce a L cuando está compuesta con K, entonces el número de todas las clases en el orden propiamente primitivo (positivo) será r veces mayor que el número de clases de orden O.

Dado que en el orden O las clases K y L pueden ser escogidas arbitrariamente, es permisible tomar clases idénticas y será particularmente ventajoso escoger aquella clase que contenga a la forma más simple de este orden. Si, por esta razón, escogemos aquella clase para K y L, la operación se verá reducida a asignar todas las clases propiamente primitivas que producen a K misma cuando estén compuestas con K. Desarrollaremos este método en lo que sigue.

254.

Teorema. *Si $F=(A, B, C)$ es la forma más simple de orden O y de determinante D, y $f=(a, b, c)$ es una forma propiamente primitiva del mismo determinante: entonces el número A^2 puede ser representado por esta forma siempre y cuando F resulte de la composición de las formas f y F; y recíprocamente F estará compuesta por sí misma y f si A^2 puede ser representada por f.*

Demostración. I. Si F es transformada en el producto $f\,F$ por la sustitución

p, p', p'', p'''; q, q', q'', q''' luego, por el artículo 235, tendremos

$$A(aq''^2 - 2bqq'' + cq^2) = A^3$$

y por ende

$$A^2 = aq''^2 - 2bqq'' + cq^2 \qquad Q.\ E.\ P.$$

II. *Presumiremos* que A^2 puede ser representado por f y designaremos los valores desconocidos por medio de los cuales es hecho esto como q'', $-q$; esto es, $A^2 = aq''^2 - 2bqq'' + cq^2$. Seguidamente póngase que

$$\begin{array}{lll} q''a - q(b+B) = Ap, & -qC = Ap', & q''(b-B) - qc = Ap'' \\ -q''C = Ap''', & q''a - q(b-B) = Aq', & q''(b+B) - qc = Aq''' \end{array}$$

Es fácil confirmar que F es transformada en el producto $f\,F$ por la sustitución p, p', p'', p'''; q, q', q'', q'''. Si los números p, p', etc. son enteros entonces F estará compuesta por f y F. Ahora, de la descripción de la forma más simple, B es 0 ó $\frac{1}{2}A$, así que $\frac{2B}{A}$ es un entero; de la misma manera es claro que $\frac{C}{A}$ es también siempre un entero. De este modo $q' - p$, p', $q''' - p''$ y p''' serán enteros y sólo queda probar que p y p'' son enteros. Ahora tenemos

$$p^2 + \frac{2pqB}{A} = a - \frac{q^2C}{A}, \qquad p''^2 + \frac{2p''q''B}{A} = c - \frac{q''^2C}{A}$$

Si $B = 0$ obtenemos

$$p^2 = a - \frac{q^2C}{A}, \qquad p''^2 = c - \frac{q''^2C}{A}$$

y así p y p'' son enteros; pero si $B = \frac{1}{2}A$ tenemos

$$p^2 + pq = a - \frac{q^2C}{A}, \qquad p''^2 + p''q'' = c - \frac{q''^2C}{A}$$

y en este caso también p y p'' son enteros. De ahí que F está compuesta por f y F. *Q. E. S.*

255.

Así, el problema se ve reducido a encontrar todas las clases propiamente primitivas de determinante D cuyas formas puedan representar a A^2. Manifiestamente A^2 puede ser representado por cualquier forma cuyo primer término es A^2 ó el cuadrado de un factor de A; recíprocamente si A^2 puede ser representado por la forma f, f será transformado en una forma cuyo primer término es $\frac{A^2}{e^2}$ por la sustitución α, β, γ, δ siempre y cuando asignemos αe y γe, cuyo máximo común divisor es e, como los valores de las incógnitas. Esta forma será propiamente equivalente a la forma f si β y δ son escogidas de tal modo que $\alpha\delta - \beta\gamma = 1$. Así resulta claro que en cualquier clase que tenga formas que puedan representar a A^2, se puede encontrar formas cuyo primer término es A^2 ó el cuadrado de un factor de A. El proceso entero depende entonces de encontrar todas las clases propiamente primitivas de determinante D que contengan formas de este tipo. Hacemos esto del siguiente modo. Sean a, a', a'' etc. todos los divisores (positivos) de A; ahora encuentre todos los valores de la expresión $\sqrt{D}$ (mod. a^2) entre 0 y $a^2 - 1$ inclusive y llámelos b, b', b'', etc. Haga

$$b^2 - D = a^2 c, \qquad b'^2 - D = a^2 c', \qquad b''^2 - D = a^2 c'', \quad \text{etc.}$$

y desígnese el conjunto de formas (a^2, b, c), (a^2, b', c'), etc. por la letra V. Obviamente cada clase de determinante D que tenga una forma con primer término a^2 también debe contener alguna forma de V. De un modo similar determinamos todas las formas de determinante D con primer término a'^2 y segundo término entre 0 y $a'^2 - 1$ inclusive y designamos el conjunto con la letra V'; por una construcción similar sea V'' el conjunto de formas similares cuyo primer término es a''^2 etc. Ahora elimine de V, V', V'', etc. todas las formas que no sean propiamente primitivas y reduzca el resto a clases. Si hubiera muchas formas que pertenecen a la misma clase, retenga sólo una de ellas. De este modo tendremos todas las clases que se buscan, y la razón de este número con respecto a la unidad será la misma que la razón del número de todas las clases propiamente primitivas (positivas) con respecto al número de todas las clases en el orden O.

Ejemplo. Sea $D = -531$ y O el orden positivo derivado a partir del orden propiamente primitivo de determinante -59; su forma más simple es $(6, 3, 90)$, así que $A = 6$. Aquí a, a', a'' y a''' serán 1, 2, 3 y 6, V contendrá a la forma $(1, 0, 531)$, V' contendrá a (4, 1, 133) y (4, 3, 135), V'' a (9, 0, 59), (9, 3, 60) y (9, 6, 63), y V''' a (36, 3, 15), (36, 9, 17), (36, 15, 21), (36, 21, 27), (36, 27, 35) y (36, 33, 45). Pero de estas doce formas seis deben ser rechazadas, la segunda y la tercera de V'', la

primera, la tercera, la cuarta, y la sexta de V'''. Todas éstas son formas derivadas; todas las seis restantes pertenecen a distintas clases. De hecho el número de clases propiamente primitivas (positivas) de determinante -531 es 18; el número de clases propiamente primitivas (positivas) de determinante -59 (o el número de clases de determinante -531 derivadas de éstas) es 3, y así la razón es de 6 a 1.

256.

Esta solución se hará más clara por medio de las siguientes observaciones generales.

I. Si el orden O es derivado a partir de un orden propiamente primitivo, A^2 dividirá a D; pero si O es impropiamente primitivo o derivado a partir de un orden impropiamente primitivo, A será par, D será divisible por $\frac{1}{4}A^2$ y el cociente será $\equiv 1 \pmod 4$. Así el cuadrado de cualquier divisor de A dividirá a D o al menos a $4D$ y en el último caso el cociente será siempre $\equiv 1 \pmod 4$.

II. Si a^2 divide a D, todos los valores de la expresión $\sqrt{D} \pmod{a^2}$ que caen entre 0 y $a^2 - 1$ serán $0, a, 2a, \ldots a^2 - a$ y así a será el número de formas en V; pero entre ellas habrá sólo tantas formas propiamente primitivas como hayan números entre

$$\frac{D}{a^2}, \frac{D}{a^2} - 1, \frac{D}{a^2} - 4, \ldots \frac{D}{a^2} - (a-1)^2$$

que no tengan un divisor común con a. Cuando $a = 1$, V consistirá de sólo una forma $(1, 0, -D)$ que será siempre propiamente primitiva. Cuando a es 2 o una potencia de 2, la mitad de los a números será par, la mitad impar; por lo cual habrá $\frac{1}{2}a$ formas propiamente primitivas en V. Cuando a es cualquier otro número primo p o una potencia del número primo p, se deben distinguir tres casos: a saber, si $\frac{D}{a^2}$ no es divisible por p y no es un residuo cuadrático de p, todos estos a números serán relativamente primos a a de tal modo que todas las formas en V serán propiamente primitivas; pero si p divide a $\frac{D}{a^2}$ habrá $\frac{(p-1)a}{p}$ formas propiamente primitivas en V; finalmente si $\frac{D}{a^2}$ es un residuo cuadrático de p no divisible por p, habrá $\frac{(p-2)a}{p}$ formas propiamente primitivas. Todo esto puede ser demostrado sin ninguna dificultad. En general, si $a = 2^\nu p^\pi q^\chi r^\rho \ldots$ donde p, q, r etc. son números primos impares distintos,

el número de formas propiamente primitivas en V será $NPQR\ldots$, donde

$N = 1$ (si $\nu = 0$) ó $N = 2^{\nu-1}$ (si $\nu > 0$)
$P = p^{\pi}$ (si $\frac{D}{a^2}$ es un no residuo cuadrático de p) o
$P = (p-1)p^{\pi-1}$ (si $\frac{D}{a^2}$ es divisible por p) o
$P = (p-2)p^{\pi-1}$ (si $\frac{D}{a^2}$ es un residuo cuadrático de p no divisible por p)

y Q, R, etc. serán definidos de la misma manera por q, r, etc. como lo es P por p.

III. Si a^2 no divide a D, $\frac{4D}{a^2}$ será un entero y $\equiv 1 \pmod 4$ y los valores de la expresión $\sqrt{D} \pmod{a^2}$ serán $\frac{1}{2}a$, $\frac{3}{2}a$, $\frac{5}{2}a, \ldots a^2 - \frac{1}{2}a$. De ahí que el número de formas en V será a y habrá tantas propiamente primitivas entre ellas como haya números entre

$$\frac{D}{a^2} - \frac{1}{4}, \frac{D}{a^2} - \frac{9}{4}, \frac{D}{a^2} - \frac{25}{4}, \ldots \frac{D}{a^2} - \left(a - \frac{1}{2}\right)^2$$

que son relativamente primos a a. Toda vez que $\frac{4D}{a^2} \equiv 1 \pmod 8$, todos estos números serán pares y así no habrá ninguna forma propiamente primitiva en V; pero cuando $\frac{4D}{a^2} \equiv 5 \pmod 8$, todos estos números serán impares, de modo que todas las formas en V serán propiamente primitivas si a es 2 o una potencia de 2. En este caso, como una norma general, habrá tantas formas propiamente primitivas en V como haya números no divisibles por algún divisor primo impar de a. Habrá $NPQR\ldots$ de ellas si $a = 2^{\nu}p^{\pi}q^{\chi}r^{\rho}\ldots$. Aquí $N = 2^{\nu}$ y P, Q, R, etc. serán derivados a partir de p, q, r, etc. de la misma manera que en el caso precedente.

IV. Hemos, por tanto, mostrado cómo determinar el número de formas propiamente primitivas en V, V', V'', etc. Podemos encontrar el número total por medio de la siguiente regla general. Si $A = 2^{\nu}\mathfrak{A}^{\alpha}\mathfrak{B}^{\beta}\mathfrak{C}^{\gamma}\ldots$, donde $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. son números primos impares distintos, el número total de todas las formas propiamente primitivas en V, V', V'', etc. será $= \frac{A\mathfrak{n}\mathfrak{a}\mathfrak{b}\mathfrak{c}\cdots}{2\mathfrak{A}\mathfrak{B}\mathfrak{C}\cdots}$ donde

$\mathfrak{n} = 1$ (si $\frac{4D}{A^2} \equiv 1 \pmod 8$), o
$\mathfrak{n} = 2$ (si $\frac{D}{A^2}$ es un entero), o
$\mathfrak{n} = 3$ (si $\frac{4D}{a^2} \equiv 5 \pmod 8$); y
$\mathfrak{a} = \mathfrak{A}$ (si $\mathfrak{A}$ divide a $\frac{4D}{A^2}$), o
$\mathfrak{a} = \mathfrak{A} \pm 1$ (si $\mathfrak{A}$ no divide a $\frac{4D}{A^2}$; el signo superior e inferior se toma de acuerdo a si $\frac{4D}{A^2}$ es un no residuo o un residuo de $\mathfrak{A}$)

Finalmente, $\mathfrak{b}$, $\mathfrak{c}$, etc. serán derivados a partir de $\mathfrak{B}$, $\mathfrak{C}$, etc. de la misma manera que $\mathfrak{a}$ a partir de $\mathfrak{A}$. La brevedad no nos permite demostrar esto más completamente.

V. Ahora, con relación al número de clases que resultan de las formas propiamente primitivas en V, V', V'', etc., debemos distinguir entre los tres casos siguientes.

Primero, cuando D es un número negativo, cada una de las formas propiamente primitivas en V, V', etc. constituye una clase separada. Por eso el número de clases será expresado por la fórmula dada en la observación previa excepto por dos casos, más exactamente cuando $\frac{4D}{A^2}$ es $= -4$ ó $= -3$; esto es, cuando D es $= -A^2$ ó $= -\frac{3}{4}A^2$. Para probar este teorema solamente debemos mostrar que es imposible para dos formas de V, V', V'', etc. distintas, el ser propiamente equivalentes. Supongamos, por tanto, que $(h^2,\ i,\ k)$, $(h'^2,\ i',\ k')$ son dos formas propiamente primitivas de V, V', V'', etc., y ambas pertenecen a la misma clase. Y supongamos que la primera es transformada en la última por medio de la sustitución propia α, β, γ, δ; obtendremos las ecuaciones

$$\alpha\delta - \beta\gamma = 1, \qquad h^2\alpha^2 + 2i\alpha\gamma + k\gamma^2 = h'^2,$$
$$h^2\alpha\beta + i(\alpha\delta + \beta\gamma) + k\gamma\delta = i'$$

De esto es fácil concluir, *primero*, que γ ciertamente no es $= 0$ (y se sigue que $\alpha = \pm 1$, $h^2 = h'^2$, $i' \equiv i \pmod{h^2}$, y las formas propuestas son idénticas, contrario a la hipótesis); *segundo*, que γ es divisible por el máximo común divisor de los números h, h' (pues si hacemos este divisor $= r$, manifiestamente también éste divide a $2i$, $2i'$ y es relativamente primo a k; además, r^2 divide a $h^2k - h'^2k' = i^2 - i'^2$; obviamente entonces r debe también dividir a $i - i'$; pero $\alpha i' - \beta h'^2 = \alpha i + \gamma k$ de modo que γk y γ también serán divisibles por r); *tercero*, $(\alpha h^2 + \gamma i)^2 - D\gamma^2 = h^2h'^2$. Si de ahí hacemos $\alpha h^2 + \gamma i = rp$, $\gamma = rq$, p y q serán enteros y q no será $= 0$ y tendremos $p^2 - Dq^2 = \frac{h^2h'^2}{r^2}$. Pero $\frac{h^2h'^2}{r^2}$ es el menor número divisible por ambos h^2 y h'^2 y, por ende, dividirá a A^2 y a $4D$. Como resultado $\frac{4Dr^2}{h^2h'^2}$ será un entero (negativo). Si lo hacemos $= -e$ tenemos $p^2 - Dq^2 = -\frac{4D}{e}$ o $4 = (\frac{2rp}{hh'})^2 + eq^2$, en esta ecuación $(\frac{2rp}{hh'})^2$ es necesariamente un cuadrado menor que 4 y así será ó 0 ó 1. En el primer caso $eq^2 = 4$ y $D = -(\frac{hh'}{rq})^2$ y se sigue que $\frac{4D}{A^2}$ es un cuadrado con signo negativo y, por ello, ciertamente no es $\equiv 1 \pmod{4}$ y de ahí que O no es un orden impropiamente primitivo ni derivado de un orden impropiamente primitivo. Así que $\frac{D}{A^2}$ será un entero, y claramente e será divisible por 4, $q^2 = 1$, $D = -(\frac{hh'}{r})^2$ y $\frac{A^2}{D}$ es también

un entero. Por esta razón, $D = -A^2$ ó $\frac{D}{A^2} = -1$, que es la primera excepción. En el último caso $eq^2 = 3$ de modo que $e = 3$ y $4D = -3(\frac{hh'}{r})^2$. Así que $3(\frac{hh'}{rA})^2$ será un entero, y no puede ser otra cosa que 3, dado que cuando lo multiplicamos por el entero cuadrado $(\frac{rA}{hh'})$ obtenemos 3. Por todo esto, $4D = -3A^2$ ó $D = -\frac{3}{4}A^2$ que es la segunda excepción. En todos los casos restantes todas las formas propiamente primitivas en V, V', V'', etc. pertenecerán a distintas clases. Para los casos de excepción es suficiente dar el resultado que puede encontrarse sin dificultad, pero es demasiado largo para presentarlo aquí. En el primer caso siempre habrá un par de formas propiamente primitivas en V, V', V'', etc. que pertenecen a la misma clase; en el último caso, habrá una terna. De modo que en el primer caso el número de clases será la mitad del valor dado arriba, en el último caso será un tercio.

Segundo, cuando D es un número cuadrado positivo, cada forma propiamente primitiva en V, V', V'', etc. constituye una clase separada sin excepción. Pues, supongamos que (h^2, i, k), (h'^2, i', k') son dos de tales formas distintas propiamente equivalentes y la primera es transformada en la última por medio de la sustitución propia α, β, γ, δ. Obviamente todos los argumentos que usamos en el caso previo, cuando no supusimos a D negativo, valen aquí. De ahí que si determinamos p, q, r como arriba, $\frac{4Dr^2}{h^2h'^2}$ será un entero aquí también, pero positivo en lugar de negativo y más aún, será un cuadrado. Si lo hacemos $= g^2$ tendremos $(\frac{2rp}{h'^2})^2 - g^2q^2 = 4$. *Q. E. A.* , debido a que la diferencia de dos cuadrados no puede ser 4 a no ser que el menor sea 0; entonces nuestra suposición es inconsistente.

Tercero, adonde D sea positivo pero no un cuadrado no tenemos aún una regla general para comparar el número de formas propiamente primitivas en V, V', V'', etc. con el número de clases diferentes que resultan de ellas. Sólo podemos decir que el último o es igual al primero o es un factor de éste. También hemos descubierto una conexión entre el cociente de estos números y los valores mínimos de t y u que satisfagan la ecuación $t^2 - Du^2 = A^2$, pero tomaría mucho explicarla aquí. No podemos decir con certeza si es posible conocer este cociente en todos los casos simplemente inspeccionando los números D y A (como en los casos previos). Damos algunos ejemplos y el lector puede añadir algunos suyos. Para $D = 13$, $A = 2$ el número de formas propiamente primitivas en V etc. es 3, todas las cuales son equivalentes y por ende conforman una clase simple; para $D = 37$, $A = 2$ también habrá tres formas propiamente primitivas en V etc. que pertenecerán a tres clases diferentes; para $D = 588$, $A = 7$ tenemos ocho formas propiamente primitivas en V etc., y ellas conforman cuatro clases; para $D = 867$, $A = 17$ habrá 18 formas

propiamente primitivas, y el mismo número para $D = 1445$, $A = 17$, pero para el primer determinante se dividirán en dos clases mientras que en el segundo habrá seis.

VI. De la aplicación de esta teoría general al caso donde O es un orden impropiamente primitivo, encontramos que el número de clases contenido en este orden posee la misma razón con respecto al número de todas las clases en el orden propiamente primitivo como 1 lo hace con respecto al número de clases propiamente primitivas distintas producido por las tres formas $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$. Ahora, cuando $D \equiv 1 \pmod 8$, habrá sólo una clase puesto que en este caso la segunda y la tercera formas son impropiamente primitivas; pero cuando $D \equiv 5 \pmod 8$ estas tres formas serán todas propiamente primitivas y producirán el mismo número de distintas clases si D es negativo excepto cuando $D = -3$, en cuyo caso habrá sólo una; finalmente, cuando D es positivo (de la forma $8n+5$) tenemos uno de los casos para el cual no hay regla general. Pero podemos decir que en este caso las tres formas pertenecerán a tres distintas clases o a una sola clase, nunca a dos; pues es fácil ver que si las formas $(1, 0, -D)$, $(4, 1, \frac{1-D}{4})$, $(4, 3, \frac{9-D}{4})$ pertenecen respectivamente a las clases K, K', K'', tendremos $K + K' = K'$, $K' + K' = K''$ y así si K y K' son idénticas, K' y K'' también serán idénticas; similarmente si K y K'' son idénticas, K' y K'' también lo serán; finalmente, dado que tendremos $K' + K'' = K$, si suponemos que K' y K'' son idénticas, se sigue que K y K' coincidirán. Así las tres clases K, K', K'' serán o todas distintas o todas idénticas. Por ejemplo, hay 75 números de la forma $8n + 5$ menores que el número 600. Entre ellos hay 16 determinantes para los cuales el caso anterior se aplica; esto es, el número de clases en el orden propiamente primitivo es de tres multiplicado por el número de clases en el orden impropiamente primitivo, o sea, 37, 101, 141, 189, 197, 269, 325, 333, 349, 373, 381, 389, 405, 485, 557, 573; para los otros 59 casos el número de clases es el mismo en ambos órdenes.

VII. Es escasamente necesario observar que el método precedente se aplica no sólo a los números de clases en órdenes distintos del mismo determinante, sino también a determinantes distintos, siempre que su cociente sea un número cuadrado. Por tanto si O es un orden de determinante dm^2, y O' un orden de determinante dm'^2, O puede ser comparado con un orden propiamente primitivo de determinante dm^2, y éste con un orden derivado a partir de un orden propiamente primitivo de determinante d; o, lo que viene a ser lo mismo, respecto al número de clases, con este último orden en sí; y en una manera similar el orden O' puede ser comparado con este mismo orden.

Sobre el número de clases ambiguas.

257.

Entre todas las clases en un orden dado con determinante dado, las clases ambiguas especialmente demandan un tratamiento mayor, y la determinación del número de clases abre la vía a varios otros resultados interesantes. Es suficiente considerar el número de clases en el orden propiamente primitivo solamente, dado que los otros casos pueden ser fácilmente reducidos a éste. Haremos esto de la siguiente manera. Primero determinaremos todas las formas propiamente primitivas ambiguas (A, B, C) de determinante D para las cuales ya sea $B = 0$ ó $B = \frac{1}{2}A$ y, entonces, a partir del número de éstos podemos encontrar el número de todas las clases propiamente primitivas ambiguas con determinante D.

I. Se encuentran todas las formas propiamente primitivas $(A, 0, C)$ de determinante D, tomando por A a cada divisor de D (ambos positivos y negativos) para el cual $C = -\frac{D}{A}$ es relativamente primo a A. De esta manera cuando $D = -1$ habrá dos de estas formas: $(1, 0, 1)$, $(-1, 0, -1)$; y el mismo número cuando $D = 1$, sean éstas $(1, 0, -1)$, $(-1, 0, 1)$; cuando D es un número primo o la potencia de un número primo (ya sea el signo positivo o negativo), habrá cuatro $(1, 0, -D)$, $(-1, 0, D)$, $(D, 0, -1)$, $(-D, 0, 1)$. En general, cuando D es divisible por n números primos distintos (aquí contamos al número 2 entre ellos), se darán en total 2^{n+1} formas de este tipo; es decir si $D = \pm PQR\ldots$ donde P, Q, R, etc. son números primos diferentes o potencias de primos y si su número $= n$, los valores de A serán 1, P, Q, R, etc. y los productos de todas las combinaciones de estos números. Por la teoría de combinaciones, el número de estos valores es 2^n, pero debe ser doblado dado que cada valor debe ser tomado con un signo positivo y un signo negativo.

II. Similarmente es claro que todas las formas propiamente primitivas $(2B, B, C)$ de determinante D serán obtenidas si por B tomamos todos los divisores (positivos y negativos) de D para los cuales $C = \frac{1}{2}(B - \frac{D}{B})$ es un entero y es relativamente primo a $2B$. Dado que de ahí C es necesariamente impar y $C^2 \equiv 1$ (mod. 8), a partir de la ecuación $D = B^2 - 2BC = (B - C)^2 - C^2$ se sigue que D o es $\equiv 3$ (mod. 4) cuando B es impar, ó $\equiv 0$ (mod. 8) cuando B es par; toda vez que, por esto, D sea congruente (mod. 8) con alguno de los números 1, 2, 4, 5, 6 no habrá ninguna forma de este tipo. Cuando $D \equiv 3$ (mod. 4), C será un entero e impar, no importa cual divisor de D tomemos por B; pero a razón de que C no tenga un divisor en común con $2B$, debemos escoger a B de tal manera que $\frac{D}{B}$ y B sean relativamente primos; así para $D = -1$ tenemos dos formas $(2, 1, 1)$, $(-2, -1, -1)$, y en general si el número de todos los divisores primos de D es n, habrá

2^{n+1} formas en total. Cuando D es divisible por 8, C será un entero si tomamos por B a cualquier divisor par de $\frac{1}{2}D$; en tanto para la otra condición, de que $C = \frac{1}{2}B - \frac{D}{2B}$ sea relativamente primo a $2B$, se satisfacerá *primero* tomando por B a todos los divisores $\equiv 2 \pmod 4$ de D para los cuales $\frac{D}{B}$ y B no tengan un divisor en común. El número de éstos (contando a ambos signos) será 2^{n+1} si D es divisible por n números primos impares distintos. *Segundo*, se toma por B a todos los divisores $\equiv 0 \pmod 4$ de $\frac{1}{2}D$ para los cuales $\frac{D}{2B}$ y B son relativamente primos. Su número también será 2^{n+1}, de modo que en este caso tendremos 2^{n+2} formas en total. Por esto, si $D = \pm 2^{\mu} PQR \ldots$ donde μ es un exponente mayor que 2, P, Q, R, etc. son números primos impares diferentes o potencias de números primos, y si el número de éstos es n: entonces *tanto* para $\frac{1}{2}B$ *como* para $\frac{D}{2B}$ se pueden tomar todos los valores 1, P, Q, R, etc. y los productos de cualquier número de estos números, cada uno con un signo positivo o un signo negativo.

A raíz de todo esto vemos que si D es divisible por n números impares primos distintos (siendo $n = 0$ cuando $D = \pm 1$ ó ± 2 ó una potencia de 2), el número de todas las formas propiamente primitivas (A, B, C) para las cuales B es, ya sea 0 ó $\frac{1}{2}A$, será 2^{n+1} cuando $D \equiv 1$ ó $\equiv 5 \pmod 8$; será 2^{n+2} cuando $D \equiv 2$, 3, 4, 6, ó $7 \pmod 8$; finalmente será 2^{n+3} cuando $D \equiv 0 \pmod 8$. Si comparamos este resultado con lo que encontramos en el artículo 231 con respecto al número de todos los caracteres posibles de las formas primitivas con determinante D, observamos que el primer número es precisamente el doble de éste en todos los casos. Pero es claro que, cuando D es negativo, habrá tantas formas positivas como negativas entre ellas.

258.

Todas las formas consideradas en el artículo previo pertenecen manifiestamente a las clases ambiguas. Por otro lado, al menos una de estas formas debe ser contenida en cada clase ambigua propiamente primitiva de determinante D; pues, ciertamente, hay formas ambiguas en tal clase y toda forma ambigua propiamente primitiva (a, b, c) de determinante D es equivalente a alguna de las formas del artículo anterior, a saber, o

$$\left(a,\, 0,\, -\frac{D}{a}\right) \qquad \text{o} \qquad \left(a,\, \frac{1}{2}a,\, \frac{1}{4}a - \frac{D}{a}\right)$$

según b sea $\equiv 0$ ó $\equiv \frac{1}{2}a \pmod a$. De este modo, el problema se reduce a encontrar cuántas clases son determinadas por estas formas.

Si la forma $(a,\ 0,\ c)$ aparece entre las formas del artículo precedente, la forma $(c,\ 0,\ a)$ también aparecerá y ellas serán distintas, excepto cuando $a = c = \pm 1$ y luego $D = -1$, un caso que dejaremos a un lado, por el momento. Ahora, dado que estas formas pertenecen manifiestamente a la misma clase, es suficiente retener una, y rechazaremos aquélla cuyo primer término es mayor que el tercero; también dejaremos a un lado el caso donde $a = -c = \pm 1$ y $D = 1$. De esta manera, podemos reducir todas las formas $(A,\ 0,\ C)$ a la mitad, reteniendo sólo una de cada par; y en aquéllas que restan siempre resulta $A < \sqrt{\pm D}$.

Similarmente, si la forma $(2b,\ b,\ c)$ aparece entre las formas del artículo previo, lo siguiente también aparecerá

$$(4c - 2b,\ 2c - b,\ c) = \left(-\frac{2D}{b},\ -\frac{D}{b},\ c\right)$$

Estas dos serán propiamente equivalentes, pero diferentes entre sí, excepto en el caso que hemos omitido, donde $c = b = \pm 1$ ó $D = -1$. Es suficiente retener aquélla, de estas dos formas, cuyo primer término es menor que el primer término de la otra (en este caso no pueden ser iguales en magnitud pero diferentes en signo). De modo que todas las formas $(2B,\ B,\ C)$ pueden ser reducidas a la mitad, rechazando una de cada par; y en aquéllas que quedan siempre tendremos $B < \frac{D}{B}$ ó $B < \sqrt{\pm D}$. De acuerdo con esto, permanece sólo la mitad de todas las formas del artículo previo. Designaremos el conjunto con la letra W, y sólo resta mostrar cuántas clases diferentes surgen a partir de estas formas. Manifiestamente, en el caso cuando D es negativo habrá tantas formas positivas en W como negativas.

I. Cuando D es negativo, cada una de las formas en W pertenecerá a una clase distinta. Pues todas las formas $(A,\ 0,\ C)$ se verán reducidas; y todas las formas $(2B,\ B,\ C)$ serán reducidas, excepto aquéllas para las cuales $C < 2B$; pues en tal forma $2C < 2B + C$; luego (dado que $B < \frac{D}{B}$, eso es $B < 2C - B$, y que $2B < 2C$ o sea $B < C$), $2C - 2B < C$ y $C - B < \frac{1}{2}C$ y la forma reducida es $(C,\ C - B,\ C)$, la cual obviamente es equivalente a ésta. De esta manera habrá tantas formas reducidas como formas haya en W, y dado que cualesquiera dos de ellas no serán idénticas u opuestas (excepto para el caso donde $C - B = 0$, en el cual $B = C = \pm 1$ y por ende $D = 1$, que es el caso que habíamos dejado de lado), todas pertenecerán a clases distintas. Así, el número de todas las clases ambiguas propiamente primitivas de determinante D será igual al número de formas en W ó a la mitad del número de formas en el artículo previo. Con respecto al caso exceptuado, cuando $D = -1$, ocurre lo mismo por compensación; esto es, hay dos clases; una a la cual pertenecen las formas $(1,\ 0,\ 1)$,

(2, 1, 1), la otra a la cual pertenecen (−1, 0, −1), (−2, −1, −1). En general, por todo esto, para un determinante negativo, el número de todas las clases ambiguas propiamente primitivas es igual al número de todos los caracteres asignables de las formas primitivas de este determinante; el número de clases ambiguas propiamente primitivas que son positivas será la mitad de éste.

II. Cuando D es un cuadrado positivo $= h^2$, no es difícil mostrar que cada forma en W pertenece a una clase diferente; pero este problema puede ser resuelto más simplemente de la siguiente manera. Por el artículo 210, debe haber una forma reducida $(a, h, 0)$ contenida en cada clase ambigua propiamente primitiva de determinante h^2, donde a es el valor de la expresión $\sqrt{1} \pmod{2h}$, que cae entre 0 y $2h-1$ inclusive. Dado que esto es así, resulta claro que hay tantas clases ambiguas propiamente primitivas de determinante h^2 como hay valores para esta expresión. Del artículo 105, el número de estos valores es 2^n, 2^{n+1} o 2^{n+2}, dependiendo de si h es impar, o $\equiv 2 \pmod 4$ o $\equiv 0 \pmod 4$; esto es, según sea $D \equiv 1$, $\equiv 4$ o $\equiv 0 \pmod 8$ donde n designa al número de divisores primos impares de h o de D. De este modo, el número de clases ambiguas propiamente primitivas será siempre la mitad del número de formas consideradas en el artículo previo e igual al número de formas en W, o sea, el número de todos los posibles caracteres.

III. Cuando D es un entero positivo no cuadrado, deduciremos, a partir de cada una de las formas (A, B, C) en W a otras formas (A', B', C'), tomando a $B' \equiv B \pmod A$, que está entre los límites $\sqrt{D}$ y $\sqrt{D} \mp A$ (el signo superior o inferior será usado según sea A positivo o negativo), y $C' = \frac{B'^2 - D}{A}$; designaremos este conjunto con la letra W'. Manifiestamente, estas formas serán propiamente primitivas y ambiguas de determinante D, todas distintas, y, más aún, todas serán formas reducidas. Pues cuando $A < \sqrt{D}$, B' será $< \sqrt{D}$ y positivo; además, $B' > \sqrt{D} \mp A$ y $A > \sqrt{D} - B'$ y luego A, tomado positivamente, cae entre $\sqrt{D} + B'$ y $\sqrt{D} - B'$. Cuando $A > \sqrt{D}$, no se puede tener $B = 0$ (habíamos rechazado estas formas), pero B debe ser $= \frac{1}{2}A$. De ahí que B' será igual, en magnitud, a $\frac{1}{2}A$ y de signo positivo (pues dado que $A < 2\sqrt{D}$, $\pm\frac{1}{2}A$ caerá entre los límites asignados a B' y será congruente con B según el modulo A; así $B' = \pm\frac{1}{2}A$). Como resultado $B' < \sqrt{D}$ y $2B' < \sqrt{D} + B'$, o bien, $A < \sqrt{D} + B'$, de tal modo que $\pm A$ necesariamente caerá entre los límites $\sqrt{D} + B'$ y $\sqrt{D} - B'$. Finalmente W' contendrá a todas las formas reducidas ambiguas propiamente primitivas de determinante D; pues si (a, b, c) es de esta forma, resultará, ya sea $b \equiv 0$ ó $b \equiv \frac{1}{2}a \pmod a$. En el primer caso, no se puede tener $b < a$, ni por esto último $a > \sqrt{D}$, así que la forma $(a, 0, -\frac{D}{a})$ ciertamente estará contenida en W y la forma correspondiente (a, b, c) en W'; en el último caso,

ciertamente $a < 2\sqrt{D}$ y, por ende, $(a,\ \frac{1}{2}a,\ \frac{1}{4}a - \frac{D}{a})$ estará contenida en W y la forma correspondiente $(a,\ b,\ c)$ en W'. Así, el número de formas en W es igual al número de todas las formas reducidas ambiguas propiamente primitivas de determinante D; pues, dado que cada clase ambigua contiene un *par* de formas reducidas ambiguas (art. 187, 194), el número de todas las clases ambiguas propiamente primitivas de determinante D será la mitad del número de formas en W, ó bien, la mitad del número de todos los caracteres posibles.

259.

El número de clases ambiguas impropiamente primitivas de un determinante D dado es igual al número de ellas propiamente primitivas del mismo determinante. Sea K la clase principal y K', K'', etc. las restantes clases ambiguas propiamente primitivas del mismo determinante; sea L una clase ambigua impropiamente primitiva del mismo determinante, p. ej. aquélla que contiene a la forma $(2,\ 1,\ \frac{1}{2} - \frac{1}{2}D)$. Si componemos la clase L con K, obtenemos la clase L misma; supongamos que la composición de la clase L con K', K'', etc. produce las clases L', L'', etc. respectivamente. Manifiestamente, todas ellas pertenecerán al mismo determinante y serán impropiamente primitivas y ambiguas. Es claro que el teorema será probado tan pronto como probemos que todas las clases L, L', L'', etc. son diferentes y que no hay otras clases ambiguas impropiamente primitivas de determinante D además de éstas. Para este propósito, distinguimos los siguientes casos.

I. Cuando el número de clases impropiamente primitivas es igual al número de clases propiamente primitivas, cada una de las primeras resultará de la composición de la clase L con una clase propiamente primitiva determinada, y así todas las L, L', L'', etc. serán diferentes. Si designamos por $\mathfrak{L}$ a cualquier clase ambigua impropiamente primitiva de determinante D, existirá una clase propiamente primitiva $\mathfrak{R}$ tal que $\mathfrak{R} + L = \mathfrak{L}$; si $\mathfrak{R}'$ es la clase opuesta a $\mathfrak{R}$, resultará también (dado que las clases L y $\mathfrak{L}$ son sus propias opuestas) $\mathfrak{R}' + L = \mathfrak{L}$, de donde necesariamente $\mathfrak{R}$ y $\mathfrak{R}'$ serán idénticas, o sea una clase ambigua. Como resultado de ésto, $\mathfrak{R}$ se encontrará entre las clases K, K', K'', etc. y $\mathfrak{L}$ entre las clases L, L', L'', etc.

II. Cuando el número de clases impropiamente primitivas es un tercio del número de clases propiamente primitivas, sea H la clase en la cual aparece la forma $(4,\ 1,\ \frac{1-D}{4})$, y H' aquélla en la cual aparece $(4,\ 3,\ \frac{9-D}{4})$. H y H' serán propiamante primitivas, distintas entre sí y de la clase principal K, y $H + H' = K$, $2H = H'$, $2H' = H$; y si $\mathfrak{L}$ es cualquier clase impropiamente primitiva de determinante D que

surge de la composición de L con la clase propiamente primitiva $\mathfrak{R}$, también se tendrá $\mathfrak{L} = L + \mathfrak{R} + H$ y $\mathfrak{L} = L + \mathfrak{R} + H'$. Además de las tres clases (propiamente primitivas y distintas) $\mathfrak{R}$, $\mathfrak{R} + H$, $\mathfrak{R} + H'$ no hay otras que produzcan a $\mathfrak{L}$ cuando se componen con L. Dado que, a raíz de esto, si $\mathfrak{L}$ es ambigua y $\mathfrak{R}'$ es opuesta a $\mathfrak{R}$, también tendremos $L + \mathfrak{R}' = \mathfrak{L}$, $\mathfrak{R}'$ será necesariamente idéntica a una de las tres clases. Si $\mathfrak{R}' = \mathfrak{R}$, $\mathfrak{R}$ será ambigua; si $\mathfrak{R}' = \mathfrak{R} + H$, resulta $K = \mathfrak{R} + \mathfrak{R}' = 2\mathfrak{R} + H = 2(\mathfrak{R} + H')$ y, por lo tanto, $\mathfrak{R} + H'$ es ambigua; similarmente, si $\mathfrak{R}' = \mathfrak{R} + H'$, $\mathfrak{R} + H$ será ambigua y concluimos que $\mathfrak{L}$ necesariamente se encuentra entre las clases L, L', L'', etc. Es fácil ver que no puede haber más de una clase ambigua entre las tres clases $\mathfrak{R}$, $\mathfrak{R} + H$, $\mathfrak{R} + H'$; pues si ambas $\mathfrak{R}$ y $\mathfrak{R} + H$ fueran ambiguas y, por lo tanto, idénticas a sus opuestas $\mathfrak{R}'$, $\mathfrak{R}' + H'$, tendríamos $\mathfrak{R} + H = \mathfrak{R} + H'$; la misma conclusión resulta a partir de la suposición de que $\mathfrak{R}$ y $\mathfrak{R} + H'$ son ambiguas; finalmente, si $\mathfrak{R} + H$ y $\mathfrak{R} + H'$ son ambiguas e idénticas con sus opuestas $\mathfrak{R}' + H'$ y $\mathfrak{R}' + H$, tendríamos $\mathfrak{R} + H + \mathfrak{R}' + H = \mathfrak{R}' + H' + \mathfrak{R} + H'$ y así $2H = 2H'$, ó bien, $H' = H$. Por esta razón, sólo habrá una clase ambigua propiamente primitiva que produce a $\mathfrak{L}$ cuando ésta es compuesta con L, y, por lo tanto, todas las L, L', L'', etc. serán diferentes.

El número de clases ambiguas en un orden *derivado* es obviamente igual al número de clases ambiguas en el orden primitivo a partir del cual es derivado, y así, este número siempre puede determinarse.

260.

PROBLEMA. *La clase propiamente primitiva K de determinante D surge a partir de la duplicación de una clase propiamente primitiva k del mismo determinante. Se buscan todas las clases similares cuya duplicación produzca a K.*

Solución. Sea H la clase principal de determinante D y sean H', H'', H''', etc. las otras clases ambiguas propiamente primitivas del mismo determinante; $k + H'$, $k + H''$, $k + H'''$, etc. son las clases que surgen a partir de la composición de éstas con k. Las designaremos como k', k'', k''', etc. Ahora bien, todas las clases k', k'', k''', etc. serán propiamente primitivas de determinante D y diferentes entre sí; y la clase K resultará de la duplicación de cualquiera de ellas. Si denotamos por $\mathfrak{R}$ a cualquier clase propiamente primitiva de determinante D que produzca a la clase K cuando sea duplicada, necesariamente estará contenida entre las clases k, k', k'', etc. Pues, supóngase que $\mathfrak{R} = k + \mathfrak{H}$, de tal modo que $\mathfrak{H}$ es una clase propiamente primitiva de determinante D (art. 249), entonces $2k + 2\mathfrak{H} = 2\mathfrak{R} = K = 2k$ y, por tanto, $2\mathfrak{H}$ coincide con la clase principal, $\mathfrak{H}$ es ambigua y, por ende, está contenida entre H,

H', H'', etc. y $\mathfrak{R}$ entre k, k', k'', etc.; por todo esto, estas clases dan una solución completa del problema.

Es evidente que, cuando D es negativo, la mitad de las clases k, k', k'', etc. serán positivas, la mitad negativas.

Dado que, a raíz de esto, toda clase propiamente primitiva de determinante D que pueda surgir a partir de la duplicación de una clase similar, proviene de la duplicación de tantas clases similares como clases ambiguas propiamente primitivas de determinante D hubiere; es claro que, si el número de todas las clases propiamente primitivas de determinante D es r, y si el número de todas las clases ambiguas propiamente primitivas de este determinante es n, entonces el número de todas las clases propiamente primitivas del mismo determinante que puede ser producido por la duplicación de una clase similar será $\frac{r}{n}$. La misma fórmula resulta si, para un determinante negativo, r y n designan los correspondientes números de clases *positivas*. De este modo, p.ej., para $D = -161$, el número de todas las clases positivas propiamente primitivas es 16, el número de clases ambiguas es 4, así que el número de clases que pueden surgir a partir de la duplicación de cualquier clase debe ser 4. De hecho, encontramos que todas las clases contenidas en el género principal están provistas de esta propiedad; por esto, la clase principal (1, 0, 161) resulta a partir de la duplicación de las cuatro clases ambiguas; (2, 1, 81) a partir de la duplicación de las clases (9, 1, 18), (9, −1, 18), (11, 2, 15), (11, −2, 15); (9, 1, 18) a partir de la duplicación de las clases (3, 1, 54), (6, 1, 27), (5, −2, 33), (10, 3, 17); finalmente (9, −1, 18) duplicando las clases (3, −1, 54), (6, −1, 27), (5, 2, 33), (10, −3, 17).

La mitad de todos los caracteres asignables para un determinante dado no puede estar en un género propiamente primitivo (positivo para un determinante negativo).

261.

TEOREMA. *La mitad de todos los caracteres asignables para un determinante positivo no cuadrado no puede pertenecer a ningún género propiamente primitivo; si el determinante es negativo, a ningún género propiamente primitivo positivo.*

Demostración. Sea m el número de todos los géneros propiamente primitivos (positivos) de determinante D; sea k el número de clases contenidas en cada género, de tal manera que km es el número de todas las clases propiamente primitivas (positivas); sea n el número de todos los caracteres diferentes asignables a este determinante. Entonces, por el artículo 258, el número de todas las clases ambiguas propiamente primitivas (positivas) será $\frac{1}{2}n$; y, por el artículo precedente, el número de todas

las clases propiamente primitivas que puedan resultar a partir de la duplicación de una clase similar será $\frac{2km}{n}$. Pero, por el artículo 247, todas estas clases pertenecen al género principal que contiene a k clases; si, por esta razón, todas las clases del género principal resultan a partir de la duplicación de alguna clase (mostraremos en lo que sigue que esto es siempre cierto), entonces $\frac{2km}{n} = k$, o bien, $m = \frac{1}{2}n$; pero es cierto que no podemos tener $\frac{2km}{n} > k$ ni, consecuentemente, $m > \frac{1}{2}n$. Dado que, por esto, el número de todos los géneros propiamente primitivos (positivos), ciertamente, no puede ser mayor que la mitad de todos los caracteres asignables, al menos la mitad de ellos no puede corresponder con tales géneros. *Q. E. D.* Nótese, sin embargo, que todavía no se sigue a partir de esto que la mitad de todos los caracteres asignables de hecho corresponden a géneros propiamente primitivos (positivos), pero luego estableceremos la validez de esta profunda proposición concerniente al misterio más recóndito de los números.

Dado que, para un determinante negativo hay siempre tantos géneros negativos como positivos, manifiestamente, no más que la mitad de todos los caracteres asignables pueden pertenecer a los géneros propiamente primitivos negativos. Hablaremos de esto y de géneros impropiamente primitivos abajo. Finalmente, observamos que el teorema no se aplica a determinantes cuadrados positivos. Por esto, es fácil ver que cada carácter asignable corresponde a un género.

Una segunda demostración del teorema fundamental y de los demás teoremas acerca de los residuos -1, $+2$, -2.

262.

Así pues, en el caso donde sólo dos caracteres diferentes pueden ser asignados a un determinante no cuadrado dado D, sólo uno corresponderá a un género propiamente primitivo (positivo) (éste tiene que ser el género principal). El otro no corresponderá a ninguna forma propiamente primitiva (positiva) de ese determinante. Esto ocurre para los determinantes -1, 2, -2, -4, para números positivos primos de la forma $4n + 1$, para negativos de primos de la forma $4n + 3$, para todas las potencias positivas impares de números primos de la forma $4n + 1$, y para potencias pares positivas o impares negativas de números primos de la forma $4n+3$. A partir de este principio, podemos desarrollar un nuevo método, no solamente para el teorema fundamental, sino también para demostrar los otros teoremas de la sección previa que tengan que ver con los residuos -1, $+2$, -2. Este método será completamente diferente de aquéllos usados en la sección anterior y, de ninguna manera, menos

elegante. Sin embargo, omitiremos la consideración del determinante -4 y de los determinantes que son potencias de números primos, dado que no nos enseñarían nada nuevo.

Para el determinante -1, no hay forma positiva con el carácter 3, 4; para el determinante $+2$ no hay ninguna con el carácter 3 *y* 5, 8; para el determinante -2 no habrá forma positiva con el carácter 5 *y* 7, 8; y para el determinante $-p$, donde p es un número primo de la forma $4n+3$, ninguna forma propiamente primitiva (positiva) tendrá al carácter Np; mientras que para el determinante $+p$, donde p es un número primo de la forma $4n+1$, ninguna forma propiamente primitiva tendrá al carácter Np. De este modo, demostraremos los teoremas de la sección previa de la siguiente manera.

I. -1 es un no residuo de cualquier número (positivo) de la forma $4n+3$. Pues si -1 fuera un residuo de tal número A, al tomar $-1 = B^2 - AC$, (A, B, C) sería una forma positiva de determinante -1 con el carácter 3, 4.

II. -1 es un residuo de cualquier número primo p de la forma $4n+1$. Pues el carácter de la forma $(-1, 0, p)$, así como de todas las formas propiamente primitivas de determinante p, será Rp y, por tanto, $-1Rp$.

III. Ambos $+2$ y -2 son residuos de cualquier número primo p de la forma $8n+1$. Pues cualquiera de las formas $(8, 1, \frac{1-p}{8})$, $(-8, 1, \frac{p-1}{8})$, o bien, las formas $(8, 3, \frac{9-p}{8})$, $(-8, 3, \frac{p-9}{8})$ son propiamente primitivas (según sea n impar o par), y así su carácter será Rp; de tal manera que $+8Rp$, y $-8Rp$, y también $2Rp$, y $-2Rp$.

IV. $+2$ es un no residuo de cualquier número de la forma $8n+3$ u $8n+5$. Pues si fuera un residuo de tal número A, habría una forma (A, B, C) de determinante $+2$ con el carácter 3 *y* 5, 8.

V. Similarmente, -2 es un no residuo de cualquier número de la forma $8n+5$ u $8n+7$, pues, de otro modo, habría una forma (A, B, C) de determinante -2 con el carácter 5 *y* 7, 8.

VI. -2 es un residuo de cualquier número primo p de la forma $8n+3$. Se muestra esta proposición por dos métodos. *Primero,* dado que, por IV, $+2Np$ y, por I, $-1Np$, necesariamente tenemos $-2Rp$. La *segunda* demostración comienza con una consideración del determinante $+2p$. A raíz de éste, cuatro caracteres son asignables, y son éstos Rp, 1 *y* 3, 8; Rp, 5 *y* 7, 8; Np, 1 *y* 3, 8; Np, 5 *y* 7, 8. De éstos, al menos dos no corresponden a ningún género. Ahora bien, la forma $(1, 0, -2p)$ estará de acuerdo con el primer carácter; la forma $(-1, 0, 2p)$ con el cuarto; de ahí que el segundo y el tercero deben ser rechazados. Y dado que el carácter de la forma

$(p,\ 0,\ -2)$ relativo al número 8 es 1 *y* 3, 8, su carácter relativo a p debe ser Rp, y así $-2Rp$.

VII. $+2$ es un residuo de cualquier número primo p de la forma $8n+7$. Esto puede ser mostrado por dos métodos. *Primero,* dado que, por I y V, $-1Np$, $-2Np$, tendrá $+2Rp$. *Segundo,* dado que, ya sea $(8,\ 1,\ \frac{1+p}{8})$ o $(8,\ 3,\ \frac{9+p}{8})$ es una forma propiamente primitiva de determinante $-p$ (dependiendo de si n es par o impar), su carácter será Rp y, por lo tanto, $8Rp$ y $2Rp$.

VIII. Cualquier número primo p de la forma $4n+1$ es un no residuo de cualquier número impar q que sea un no residuo de p. Pues, claramente, si p fuera un residuo de q, habría una forma propiamente primitiva de determinante p con el carácter Np.

IX. Similarmente, si un número impar q es un no residuo de un número primo p de la forma $4n+3$, $-p$ será un no residuo de q; de cualquier otra manera, habría una forma propiamente primitiva de determinante $-p$ con el carácter Np.

X. Cualquier número primo p de la forma $4n+1$ es un residuo de cualquier otro número primo q que sea un residuo de p. Si q es también de la forma $4n+1$, esto se sigue inmediatamente a partir de VIII; pero si q es de la forma $4n+3$, $-q$ será también un residuo de p (por II) y, así, pRq (por IX).

XI. Si un número primo q es un residuo de otro número primo p de la forma $4n+3$, $-p$ será un residuo de q. Pues si q es de la forma $4n+1$, se sigue inmediatamente, a partir de VIII, que pRq y, así, (por II) $-pRq$; este método no funciona cuando q es de la forma $4n+3$, pero puede ser fácilmente resuelto considerando al determinante $+pq$. Pues, dado que, de los cuatro caracteres asignables para este determinante Rp, Rq; Rp, Nq; Np, Rq; Np, Nq, dos de ellos no pueden corresponder a cualquier género y, dado que los caracteres de las formas $(1,\ 0,\ -pq)$ y $(-1,\ 0,\ pq)$ son el primero y el cuarto, respectivamente, entonces el segundo y el tercero son los caracteres que no corresponden a ninguna forma propiamente primitiva de determinante pq. Y, dado que, por hipótesis, el carácter de la forma $(q,\ 0,\ -p)$ con respecto al número p es Rp, su carácter con respecto al número q debe ser Rq y, por ende, $-pRq$. *Q. E. D.*

Si en las proposiciones VIII y IX se supone que q es un número primo, estas proposiciones, junto con X y IX, nos darán el teorema fundamental de la sección previa.

Se determina más exactamente la mitad de los caracteres que no pueden corresponder a ningún género.

263.

Ahora que hemos dado una nueva prueba del teorema fundamental, mostramos como distinguir a la mitad de los caracteres de un determinante no cuadrado dado que no puedan corresponder a ninguna de las formas propiamente primitivas (positivas). Podemos tratar esto más brevemente, dado que la base para nuestra discusión está ya contenida en los artículos 147–150. Sea e^2 el mayor cuadrado que divide al determinante dado D, y sea $D = D'e^2$, de tal modo que D' no incluye ningún factor cuadrado. Más aún, sean a, b, c, etc. todos los divisores impares primos de D'. De manera que D', excepto quizás por su signo, será un producto de estos números o el doble de este producto. Desígnese por Ω el conjunto de caracteres particulares Na, Nb, Nc, etc., tomado por sí mismo cuando $D' \equiv 1 \pmod 4$; tomado junto con el carácter añadido 3, 4 cuando $D' \equiv 3$ y e es impar o $\equiv 2 \pmod 4$; tomado junto con 3, 8 y 7, 8 cuando $D' \equiv 3$ y $e \equiv 0 \pmod 4$; tomado ya sea junto con el carácter 3 *y* 5, 8 cuando $D' \equiv 2 \pmod 8$ y e es impar, o bien con los dos caracteres 3, 8 y 5, 8 cuando e es par; finalmente tomado ya sea junto con el carácter 5 *y* 7, 8 cuando $D' \equiv 6 \pmod 8$ y e es impar o con los dos caracteres 5, 8 y 7, 8 cuando e es par. Hecho esto, ningún género propiamente primitivo (positivo) de determinante D puede corresponder a ningún carácter completo que contenga un número impar de caracteres particulares Ω. En cada caso, los caracteres particulares, los cuales expresan una relación con aquellos divisores de D que no dividen a D', no contribuyen en nada a la posibilidad o imposibilidad de los géneros. A partir de la teoría de combinaciones, sin embargo, es fácil ver que, de esta manera, la mitad de todos los caracteres completos asignables están excluidos.

Demostramos esto de la siguiente manera. Por los principios de la sección previa, o por los teoremas que recién hemos demostrado en el artículo precedente, es claro que si p es un número primo (impar positivo) que no divide a D y que posee a uno de los caracteres rechazados correspondientes a éste, D' involucrará a un número impar de factores que son no residuos de p. De ahí que D' y D también serán no residuos de p. Más aún, el producto de números impares relativamente primos a D, ninguno de los cuales corresponde a alguno de los caracteres rechazados, no puede corresponder a un carácter cualquiera como tal. Y, recíprocamente, cualquier número impar positivo relativamente primo a D, que corresponda con uno de los caracteres rechazados, ciertamente implica algún factor primo de la misma calidad. Si, por este motivo, se da una forma propiamente primitiva (positiva) de determinante D

correspondiente a uno de los caracteres rechazados, D sería un no residuo de algún número impar positivo relativamente primo a éste y representable por tal forma. Pero esto es evidentemente inconsistente con el teorema del artículo 154.

Las clasificaciones en los artículos 231 y 232 dan buenos ejemplos de esto, y el lector puede aumentar su número a su gusto.

264.

De este modo, dado un determinante no cuadrado, todos los caracteres asignables estarán equitativamente distribuidos en dos tipos, P y Q, de tal manera que ninguna forma propiamente primitiva (positiva) puede corresponder a uno de los caracteres Q. En tanto para los caracteres P, de lo que sabemos hasta el momento, no hay nada que les impida el pertenecer a formas de esta especie. Se nota especialmente la siguiente proposición concerniente a estos tipos de caracteres, la cual puede ser fácilmente deducida a partir de los criterios concernientes a ellos. Si se compone un carácter de P con un carácter de Q (como en el artículo 246, si el carácter de Q también correspondiera a un género) se producirá un carácter de Q; pero si se componen dos caracteres de P o dos de Q, el carácter resultante pertenecerá a P. Con la ayuda de este teorema, se puede excluir también a la mitad de todos los caracteres asignables para géneros negativos e impropiamente primitivos de la siguiente manera.

I. Para un determinante negativo D, los géneros negativos serán contrarios a los géneros positivos en el sentido de que ninguno de los caracteres de P pertenecerá a un género negativo propiamente primitivo, pero todos esos géneros tendrán caracteres de Q. Pues cuando $D' \equiv 1 \pmod 4$, $-D'$ será un número positivo de la forma $4n+3$, y así, entre los números a, b, c, etc. habrá un número impar de la forma $4n+3$ y -1 será un no residuo de cada uno de ellos. Se sigue en este caso que el carácter completo de la forma $(-1, 0, D)$ incluirá un número impar de caracteres particulares de Ω y así pertenecerá a Q; cuando $D' \equiv 3 \pmod 4$, por una razón similar, entre los números a, b, c, etc. habrá, o bien ningún número de la forma $4n+3$, o bien dos o cuatro, etc. Y, dado que en este caso 3, 4 o 3, 8 o 7, 8 ocurrirán entre los caracteres particulares de la forma $(-1, 0, D)$, es claro que el carácter completo de esta forma también pertenecerá a Q. Se obtiene la misma conclusión con igual facilidad para los casos restantes de tal modo que la forma negativa $(-1, 0, D)$ siempre tendrá un carácter de Q. Pero dado que esta forma compuesta con cualquier otra forma negativa propiamente primitiva del mismo determinante producirá una forma positiva similar,

es claro que ninguna forma propiamente primitiva negativa puede tener un carácter de P.

II. Se puede probar, de la misma manera, que los géneros impropiamente primitivos (positivos) tienen, ya sea, la misma propiedad o la opuesta de los géneros propiamente primitivos, dependiendo de si $D \equiv 1$ ó $\equiv 5 \pmod 8$. Pues en el primer caso también tendremos $D' \equiv 1 \pmod 8$, y se concluye que, entre los números a, b, c, etc., o bien no habrá números de la forma $8n+3$ y $8n+5$, o bien dos de ellos, o cuatro, etc. (esto es, el producto de cualquier número de enteros impares que incluya a un número impar de enteros de la forma $8n+3$ y $8n+5$, será siempre $\equiv 3$ o $\equiv 5 \pmod 8$, y el producto de todos los números a, b, c, etc. será igual a D' o a $-D'$): de este modo, el carácter completo de la forma $(2,\ 1,\ \frac{1-D}{2})$ no involucrará a ningún carácter particular de Ω, o bien involucrará a dos o a cuatro, etc. y así pertenecerá a P. Ahora bien, dado que cualquier forma impropiamente primitiva (positiva) de determinante D puede ser considerada como si estuviera compuesta por $(2,\ 1,\ \frac{1-D}{2})$ y por una forma propiamente primitiva (positiva) del mismo determinante, es obvio que ninguna forma impropiamente primitiva (positiva) puede tener a uno de los caracteres de Q en este caso. En el otro caso, cuando $D \equiv 5 \pmod 8$, sucede lo contrario, esto es D', el cual también será $\equiv 5$, ciertamente involucrará un número impar de factores de la forma $8n+3$ y $8n+5$. De este modo, el carácter de la forma $(2,\ 1,\ \frac{1-D}{2})$, y también el carácter de cualquier forma impropiamente primitiva (positiva) de determinante D pertenecerá a Q y ningún género propiamente primitivo positivo puede tener a un carácter en P.

III. Finalmente, para un determinante negativo, los géneros negativos impropiamente primitivos son, de nuevo, contrarios a los géneros impropiamente primitivos. Ellos no pueden tener un carácter que pertenezca a P o a Q, dependiendo a si $D \equiv 1$ o $\equiv 5 \pmod 8$, o bien, dependiendo de si $-D$ es de la forma $8n+7$ u $8n+3$. Se deduce esto del hecho de que si componemos la forma $(-1,\ 0,\ D)$, cuyo carácter está en Q, con formas negativas impropiamente primitivas del mismo determinante, obtenemos formas positivas impropiamente primitivas. De este modo, cuando los caracteres de Q son excluidos de éstas, los caracteres de P deben también ser excluidos, y recíprocamente.

Un método especial para descomponer primos en dos cuadrados.

265.

Todo lo anterior está basado en las consideraciones de los artículos 257 y

258, concernientes al número de clases ambiguas. Hay muchas otras conclusiones muy dignas de atención, las cuales, para ser breve omitiremos, pero no podemos pasar sobre la siguiente, que es significativa por su elegancia. Para un determinante positivo p, que es un número primo de la forma $4n + 1$, hemos mostrado que sólo hay una clase ambigua propiamente primitiva. Así pues, todas las formas ambiguas propiamente primitivas de este determinante serán propiamente equivalentes. Si, por este motivo, b es el entero positivo inmediatemente menor que $\sqrt{p}$ y $p - b^2 = a'$, las formas $(1, b, -a')$, $(-1, b, a')$ serán propiamente equivalentes y, dado que ambas son formas reducidas, una estará contenida en el período de la otra. Si se asigna el índice 0 a la primera forma en su período, el índice de la última necesariamente será impar (dado que los primeros términos de estas dos formas tienen signos opuestos); supóngase, por tanto, que este índice es $= 2m + 1$. Es fácil ver que, si las formas de índices 1, 2, 3, etc. son respectivamente

$$(-a', b', a''), \qquad (a'', b'', -a'''), \qquad (-a''', b''', a''''), \qquad \text{etc.},$$

las siguientes formas corresponderán a los índices $2m$, $2m - 1$, $2m - 2$, $2m - 3$, etc., respectivamente:

$$(a', b, -1), \qquad (-a'', b', a'), \qquad (a''', b'', -a''), \qquad (-a'''', b''', a'''), \qquad \text{etc.}$$

Así, si la forma de índice m es (A, B, C), $(-C, B, -A)$ será la misma y, por ende, $C = -A$ y $p = B^2 + A^2$. Por esta razón, cualquier número primo de la forma $4n + 1$ puede ser descompuesto en dos cuadrados (deducimos esta proposición a partir de principios enteramente diferentes en el artículo 182). Y podemos encontrar esta descomposición por un método muy simple y completamente uniforme; esto es, mediante el cómputo del período de la forma reducida cuyo determinante es aquel número primo y cuyo primer término es 1, hacia una forma cuyos términos exteriores son iguales en magnitud pero opuestos en signo. Entonces, p.ej., para $p = 233$ tenemos $(1, 15, -8)$, $(-8, 9, 19)$, $(19, 10, -7)$, $(-7, 11, 16)$, $(16, 5, -13)$, $(-13, 8, 13)$ y $233 = 64 + 169$. Es claro que A es necesariamente impar (dado que $(A, B, -A)$ debe ser una forma propiamente primitiva) y que B es par. Dado que, para el determinante positivo p, el cual es un número primo de la forma $4n+1$, sólo una clase ambigua está contenida en el orden impropiamente primitivo, es claro que, si g es el número impar inmediatamente menor que $\sqrt{p}$ y $p - g^2 = 4h$, las formas reducidas impropiamente primitivas $(2, g, -2h)$, $(-2, g, 2h)$ serán propiamente equivalentes

y, por tanto, una estará contenida en el período de la otra. Así pues, por un razonamiento similar, se concluye que se puede encontrar una forma en el período de la forma $(2,\ g,\ -2h)$, la cual tiene términos exteriores de igual magnitud y signo opuesto. De este modo, podemos descomponer el número p en dos cuadrados. Los términos exteriores de esta forma serán pares, el de la mitad será impar; y dado que se sabe que un número primo puede ser descompuesto en dos cuadrados de sólo una manera, la forma que encontramos por este método será $(B,\ \pm A,\ -B)$ o $(-B,\ \pm A,\ B)$. Por eso, en nuestro ejemplo para $p = 233$ tendremos $(2,\ 15,\ -4)$, $(-4,\ 13,\ 16)$, $(16,\ 3,\ -14)$, $(-14,\ 11,\ 8)$, $(8,\ 13,\ -8)$ y $233 = 169 + 64$, como arriba.

UNA DIGRESION CONTENIENDO UN ESTUDIO DE FORMAS TERNARIAS.

266.

Hasta aquí hemos restringido nuestra discusión a funciones de segundo grado con *dos* incógnitas y no había necesidad de darles a ellas un nombre especial. Pero, evidentemente, este tema es sólo una sección del tratado general concerniente a las *funciones algebraicas racionales enteras y homogéneas con varias incógnitas y de varios grados.* Tales funciones, según su exponente, pueden ser apropiadamente divididas en *formas de segundo, tercero, cuarto grado, etc.*, y, según su número de incógnitas, en *formas binarias, ternarias, cuaternarias, etc.* De este modo, las formas que hemos venido considerando pueden ser llamadas simplemente *formas binarias de segundo grado.* Pero las funciones como

$$Ax^2 + 2Bxy + Cy^2 + 2Dxz + 2Eyz + Fz^2$$

(donde A, B, C, D, E y F son enteros) son llamadas *formas ternarias de segundo grado*, y así sucesivamente. Hemos dedicado la presente sección al tratamiento de formas binarias de segundo grado. Pero hay muchas verdades bellas concernientes a estas formas cuya fuente real se indaga en la teoría de formas ternarias de segundo grado. Haremos, por tanto, una breve digresión dentro de esta teoría y trataremos especialmente de aquellos elementos que son necesarios para completar la teoría de las forma binarias, esperando, gracias a esto, complacer a los geómetras quienes se desilusionarían si ignoramos esta parte o la tratáramos de una manera menos natural. Debemos, sin embargo, reservar un tratamiento más exacto de este importante tema para otra ocasión porque su utilidad sobradamente excede los límites de este trabajo y porque, con esa esperanza, seríamos capaces de enriquecer la discusión con un

desarrollo más profundo más adelante. En este momento excluiremos completamente de la discusión a las formas cuaternarias, quinarias, etc. y a todas las formas de grados más altos*). Es suficiente dirigir este ancho campo a la atención de los geómetras. Hay material amplio para el ejercicio de su genio, y la Aritmética trascendental seguramente se beneficiará con sus esfuerzos.

267.

Será de gran ventaja para nuestro entendimiento establecer un orden fijo para los valores desconocidos de la forma ternaria, justo como lo hicimos para formas binarias, de tal manera que podamos distinguir las *incógnitas primera, segunda* y *tercera* entre sí. Al disponer las distintas partes de una forma siempre observaremos el siguiente orden; fijaremos, en primer lugar, el término que involucra el cuadrado de la primera incógnita, luego el término que involucra el cuadrado de la segunda incógnita, el cuadrado de la tercera incógnita, el doble producto de la segunda por la tercera, el doble producto de la primera por la tercera, y luego el doble producto de la primera por la segunda. Finalmente, llamamos a los enteros por los cuales estos cuadrados y doble productos están multiplicados, en el mismo orden, los *coeficientes primero, segundo, tercero, cuarto, quinto,* y *sexto.* De este modo,

$$ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

será una forma ternaria correctamente ordenada. La primera incógnita es x, la segunda x', la tercera x''. El primer coeficiente es a etc., el cuarto es b etc. Pero, dado que contribuye mucho a la brevedad, si no es siempre necesario denotar las incógnitas de una forma ternaria por letras especiales, también designaremos tal forma por

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$$

Poniendo

$$\begin{array}{lll} b^2 - a'a'' = A, & b'^2 - aa'' = A', & b''^2 - aa' = A'' \\ ab - b'b'' = B, & a'b' - bb'' = B', & a''b'' - bb' = B'' \end{array}$$

*) Por esta razón, siempre que hablamos simplemente acerca de las formas binarias y ternarias, queremos decir formas binarias o ternarias de *segundo grado.*

obtendremos otra forma

$$\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix} \dots \quad F$$

a la que llamamos la *adjunta* de la *forma*

$$\begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix} \dots \quad f.$$

De nuevo, si denotamos por brevedad al número

$$ab^2 + a'b'^2 + a''b''^2 - aa'a'' - 2bb'b'' \quad \text{por} \quad D,$$

tendremos

$$\begin{array}{lll} B^2 - A'A'' = aD, & B'^2 - AA'' = a'D, & B''^2 - AA' = a''D \\ AB - B'B'' = bD, & A'B' - BB'' = b'D, & A''B'' - BB' = b''D \end{array}$$

y es obvio que la adjunta de la forma F será la forma

$$\begin{pmatrix} aD, & a'D, & a''D \\ bD, & b'D, & b''D \end{pmatrix}.$$

Las propiedades de la forma ternaria f dependen, primero, de la naturaleza del número D. Lo llamaremos el *determinante* de esta forma. De la misma manera, el determinante de la forma F será $= D^2$, esto es, igual al cuadrado del determinante de la forma f, de la cual es adjunta.

Así, p.ej., la adjunta de la forma ternaria

$$\begin{pmatrix} 29, & 13, & 9 \\ 7, & -1, & 14 \end{pmatrix} \text{ es } \begin{pmatrix} -68, & -260, & -181 \\ 217, & -111, & 133 \end{pmatrix}$$

y el determinante de cada una es $= 1$.

Excluiremos enteramente de nuestra siguiente investigación a las formas ternarias de determinante 0. Mostraremos en otro momento, cuando tratemos más completamente la teoría de formas ternarias, que éstas son formas ternarias sólo en *apariencia*. Ellas son de hecho equivalentes a formas binarias.

268.

Si una forma ternaria f de determinante D y con incógnitas x, x', x'' (la primera $= x$ etc.) es transformada en una forma ternaria g de determinante E e incógnitas y, y', y'' por medio de una sustitución tal como ésta

$$\begin{aligned} x &= \alpha y + \beta y' + \gamma y'' \\ x' &= \alpha' y + \beta' y' + \gamma' y'' \\ x'' &= \alpha'' y + \beta'' y' + \gamma'' y'' \end{aligned}$$

donde los nueve coeficientes α, β, etc. son todos enteros, entonces por brevedad, ignoraremos las incógnitas y diremos simplemente que f es transformada en g por medio de la sustitución (S)

$$\begin{array}{lll} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

y que f *implica a* g o bien que g está *contenida* en f. A partir de esta suposición se seguirán seis ecuaciones para los seis coeficientes en g, pero es innecesario transcribirlas aquí. Y a partir de éstas, resultan las siguientes conclusiones:

I. Si por brevedad denotamos al número

$$\alpha\beta'\gamma'' + \beta\gamma'\alpha'' + \gamma\alpha'\beta'' - \gamma\beta'\alpha'' - \alpha\gamma'\beta'' - \beta\alpha'\gamma'' \qquad \text{por } k$$

encontramos, luego del cálculo adecuado, que $E = k^2 D$. De este modo, D divide a E y el cociente es un cuadrado. Es claro que, con respecto a las transformaciones de formas ternarias, el número k es similar al número $\alpha\delta - \beta\gamma$ del artículo 157 con respecto a las transformaciones de formas binarias, a saber, la raíz cuadrada del cociente de los determinantes. Podemos conjeturar que, en este caso, una diferencia del signo de k indica una diferencia esencial entre transformaciones propias e impropias y sus implicaciones. Pero si examinamos la situación más de cerca, vemos que f es transformada en g por medio de esta sustitución también

$$\begin{array}{lll} -\alpha, & -\beta, & -\gamma \\ -\alpha', & -\beta', & -\gamma' \\ -\alpha'', & -\beta'', & -\gamma''. \end{array}$$

En la ecuación para k, poniendo $-\alpha$ por α, $-\beta$ por β, etc., obtendremos $-k$. De esta manera, esta sustitución sería similar a la sustitución S y cualquier forma ternaria

que implique a otra de una manera, también implicaría la misma forma de la otra manera. Así que abandonaremos enteramente esta distinción, dado que no es de ningún uso para formas ternarias.

II. Si denotamos por F y G las formas que son adjuntas a f y a g respectivamente, los coeficientes en F estarán determinados por los coeficientes en f, los coeficientes en G por los valores de los coeficientes de la forma g a partir de la ecuación que es proveida por la sustitución S. Si expresamos los coeficientes de la forma f por letras y comparamos los valores de los coeficientes de las formas F y G, es fácil ver que F implica a G y que es transformada en G por medio de la sustitución (S')

$$\begin{array}{lll} \beta'\gamma'' - \beta''\gamma', & \gamma'\alpha'' - \gamma''\alpha', & \alpha'\beta'' - \alpha''\beta' \\ \beta''\gamma - \beta\gamma'', & \gamma''\alpha - \gamma\alpha'', & \alpha''\beta - \alpha\beta'' \\ \beta\gamma' - \beta'\gamma, & \gamma\alpha' - \gamma'\alpha, & \alpha\beta' - \alpha'\beta. \end{array}$$

Dado que el cálculo no presenta ninguna dificultad, no lo escribiremos.

III. Por medio de la sustitución (S'')

$$\begin{array}{lll} \beta'\gamma'' - \beta''\gamma', & \beta''\gamma - \beta\gamma'', & \beta\gamma' - \beta'\gamma \\ \gamma'\alpha'' - \gamma''\alpha', & \gamma''\alpha - \gamma\alpha'', & \gamma\alpha' - \gamma'\alpha \\ \alpha'\beta'' - \alpha''\beta', & \alpha''\beta - \alpha\beta'', & \alpha\beta' - \alpha'\beta. \end{array}$$

g será transformada en la misma forma que f por medio de la sustitución

$$\begin{array}{lll} k, & 0, & 0 \\ 0, & k, & 0 \\ 0, & 0, & k \end{array}$$

Esta es la forma que surge de multiplicar cada uno de los coeficientes de la forma f por k^2. Designaremos esta forma por f'.

IV. Exactamente de la misma manera, probamos que, por medio de la sustitución (S''')

$$\begin{array}{lll} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{array}$$

la forma G será transformada en la forma que surge a partir de F, multiplicando cada coeficiente por k^2. Designaremos esta forma por F'.

Diremos que la sustitución S''' surge a partir de la *transposición* de la sustitución S, y, manifiestamente, obtendremos S de nuevo a partir de la transposición de la sustitución S'''; de la misma manera, cada una de las sustituciones S', S'' se produce de la transposición de la otra. Podemos llamar a la sustitución S' como la *adjunta* de la sustitución S, y la sustitución S'' será la adjunta de la sustitución S'''.

269.

Si la forma f implica a g y g también implica a f, entonces f y g se llaman formas *equivalentes*. En este caso D divide a E, pero E también divide a D y así $D = E$. En el sentido contrario, si la forma f implica a una forma g del mismo determinante, estas formas serán equivalentes. Pues (si usamos los mismos símbolos del artículo previo excepto por el caso cuando $D = 0$) tenemos $k = \pm 1$ y así la forma f', en la cual g es transformada por medio de la sustitución S'', es idéntica a f y f está contenida en g. Más aún, en este caso las formas F y G, las cuales son adjuntas a f y a g, serán equivalentes entre sí, y la última será transformada en la primera por medio de la sustitución S'''. Finalmente, en el sentido contrario, si *se supone* que las formas F y G son equivalentes y que la primera es transformada en la segunda por medio de la sustitución T, las formas f y g también serán equivalentes, y f será transformada en g por medio de la sustitución adjunta a T y g en f por medio de la sustitución que surge de la transposición de la sustitución T. Pues, por estas dos sustituciones, respectivamente, la forma adjunta a F será transformada en la forma adjunta a G y viceversa. Estas dos formas, sin embargo, vienen de f y de g al multiplicar todos los coeficientes por D; así que se concluye que f es transformada en g y g en f, respectivamente, por estas mismas sustituciones.

270.

Si la forma ternaria f implica a la forma ternaria f' y f' implica a la forma f'', entonces f también implicará a f''. Pues es fácil observar que si f es transformada en f' por medio de la sustitución

$$\begin{array}{lll} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'', \end{array}$$

y f' en f'' por medio de la sustitución

$$\begin{array}{ccc} \delta, & \varepsilon, & \zeta \\ \delta', & \varepsilon', & \zeta' \\ \delta'', & \varepsilon'', & \zeta'', \end{array}$$

entonces f será transformada en f'' por medio de la sustitución

$$\begin{array}{ccc} \alpha\delta+\beta\delta'+\gamma\delta'', & \alpha\varepsilon+\beta\varepsilon'+\gamma\varepsilon'', & \alpha\zeta+\beta\zeta'+\gamma\zeta'' \\ \alpha'\delta+\beta'\delta'+\gamma'\delta'', & \alpha'\varepsilon+\beta'\varepsilon'+\gamma'\varepsilon'', & \alpha'\zeta+\beta'\zeta'+\gamma'\zeta'' \\ \alpha''\delta+\beta''\delta'+\gamma''\delta'', & \alpha''\varepsilon+\beta''\varepsilon'+\gamma''\varepsilon'', & \alpha''\zeta+\beta''\zeta'+\gamma''\zeta''. \end{array}$$

Y en el caso donde f es equivalente a f' y f' a f'', la forma f también será equivalente a la forma f''. Es inmediatamente obvio cómo estos teoremas funcionan con una serie de varias formas.

271.

Es aparente, a partir de lo que hemos visto, que las formas ternarias, al igual que las binarias, pueden ser distribuidas en *clases*, asignando formas equivalentes a la misma clase y formas no-equivalentes a clases diferentes. Las formas con determinantes diferentes, ciertamente por lo anterior, pertenecerán a clases diferentes y, por tanto, habrá un número infinito de clases de formas ternarias. Las formas ternarias de un mismo determinante a veces producen un número grande de clases y a veces un número pequeño, pero es una propiedad importante de estas formas el que *todas las formas de un mismo determinante dado siempre constituyen un número finito de clases.* Antes de que discutamos este teorema importante en detalle, debemos explicar la siguiente diferencia esencial que se obtiene entre formas ternarias.

Ciertas formas ternarias están de tal manera construidas que pueden representar indistintamente números positivos y negativos, p.ej. la forma $x^2+y^2-z^2$. Se llamarán entonces *formas indefinidas.* Por otro lado, hay formas que no pueden representar a números negativos sino (excepto por el cero, el cual se obtiene haciendo cada incógnita $=0$) solamente números positivos, p.ej. $x^2+y^2+z^2$. Se llamarán *formas positivas.* Finalmente hay otras que no pueden representar números positivos, p.ej. $-x^2-y^2-z^2$. Estas serán llamadas *formas negativas.* Las formas positivas y negativas son ambas llamadas *formas definidas.* Ahora daremos un criterio general para determinar cómo distinguir estas propiedades de las formas.

Si se multiplica la forma ternaria

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

de determinante D por a, y si los coeficientes de la forma que es adjunta a f se denotan como en el artículo 267 por A, A', A'', B, B', B'', tenemos

$$(ax + b''x' + b'x'')^2 - A''x'^2 + 2Bx'x'' - A'x''^2 = g$$

y, multiplicando por A', obtenemos

$$A'(ax + b''x' + b'x'')^2 - (A'x'' - Bx')^2 + aDx'^2 = h.$$

Si ambos A' y aD son números negativos, todos los valores de h serán negativos, y evidentemente la forma f puede representar sólo números cuyo signo es opuesto al de aA', v.g., idénticos al signo de a u opuestos al signo de D. En este caso, f será una forma definida y será positiva o negativa, dependiendo de si a es positivo o negativo, o bien, según sea D negativo o positivo.

Pero si aD, A' son ambos positivos, o bien, uno es positivo y el otro negativo (ninguno $= 0$), h puede producir, ya sea, cantidades positivas o negativas mediante una escogencia adecuada de x, x' y x''. Así pues, en este caso f puede producir valores tanto del mismo signo como del signo opuesto a aA', y será una forma indefinida.

Para el caso donde $A' = 0$ pero a no es $= 0$, tenemos

$$g = (ax + b''x' + b'x'')^2 - x'(A''x' - 2Bx'').$$

Dándole a x' un valor arbitrario (diferente de 0) y tomando x'' de tal manera que $\frac{A''x'}{2B} - x''$ tenga el mismo signo que Bx' (esto puede lograrse dado que B no puede ser $= 0$ pues tendríamos $B^2 - A'A'' = aD = 0$, y $D = 0$, o sea el caso excluido), $x'(A''x' - 2Bx'')$ será una cantidad positiva, y luego x puede ser escogida para hacer de g una cantidad negativa. Manifiestamente todos estos valores pueden ser escogidos de tal manera que, si se desea, todos sean enteros. Finalmente, no importa qué valores sean dados a x' y a x'', x puede ser tomado tan grande como para hacer a g positiva. De modo que en este caso f será una forma indefinida.

Finalmente, si $a = 0$ resulta

$$f = a'x'^2 + 2bx'x'' + a''x''^2 + 2x(b''x' + b'x'').$$

Ahora, si tomamos x' y x'' arbitrariamente, pero de tal manera que $b''x' + b'x''$ no sea $= 0$ (obviamente esto puede hacerse a menos que ambos b' y b'' sean $= 0$; pero entonces tendríamos $D = 0$), es fácil ver que x puede ser escogido de tal modo que f tendrá tanto valores positivos como negativos. Y en este caso también f será una forma indefinida.

De la misma manera que determinamos la propiedad de la forma f a partir de los números aD y A', también pueden usarse aD y A'', de modo que la forma f sea definida si ambos aD y A'' son negativos; indefinida en todos los otros casos. Se puede, para el mismo propósito, considerar los números $a'D$ y A, o bien $a'D$ y A'', o bien $a''D$ y A, o finalmente $a''D$ y A'.

A raíz de todo esto se sigue que, en una forma definida, los seis números A, A', A'', aD, $a'D$ y $a''D$ son todos negativos. Para la forma positiva, a, a' y a'' serán positivos y D negativo; para la forma negativa, a, a' y a'' serán negativos y D positivo. De ahí que todas las formas ternarias con un determinante positivo dado pueden ser distribuidas en formas negativas y formas indefinidas; todas aquéllas con un determinante negativo, en formas positivas y formas indefinidas; y no hay formas positivas con un determinante positivo ni formas negativas con un determinante negativo. Y es fácil ver que la adjunta de una forma definida es siempre definida y *negativa*, y la adjunta de una forma indefinida es siempre indefinida.

Dado que todos los números que son representables por una forma ternaria dada pueden también ser representados por todas las formas que son equivalentes a ella, las formas ternarias de la misma clase son todas indefinidas o todas positivas o todas negativas. Así es legítimo transferir estas designaciones también a clases enteras.

272.

Trataremos el teorema propuesto en el artículo previo, el cual dice que todas las formas ternarias de un determinante dado pueden ser distribuidas en un número *finito* de clases, por un método análogo al que usamos en el caso de las formas binarias. Primero mostraremos cómo cada forma ternaria puede ser reducida a una forma más simple y luego mostraremos que el número de las formas más simples (que resulta de tales reducciones) es finito para un determinante dado. Supongamos, en general, que la forma dada es la forma ternaria $f = \begin{pmatrix} a, & a', & a'' \\ b, & b', & b'' \end{pmatrix}$ de determinante D (diferente

de cero) y que es transformada en la forma equivalente $g = \begin{pmatrix} m, & m', & m'' \\ n, & n', & n'' \end{pmatrix}$ por medio de la sustitución (S):

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma''. \end{matrix}$$

Nos resta determinar α, β, γ, etc. de tal modo que g sea más simple que f. Sean $\begin{pmatrix} A, & A', & A'' \\ B, & B', & B'' \end{pmatrix}$, $\begin{pmatrix} M, & M', & M'' \\ N, & N', & N'' \end{pmatrix}$ las formas adjuntas a f y g respectivamente, y designémoslas por F y G. Entonces, por el artículo 269, F será transformada en G por medio de una sustitución que es adjunta a S, y G será transformada en F por medio de una sustitución derivada de la transposición de S. El número

$$\alpha\beta'\gamma'' + \alpha'\beta''\gamma + \alpha''\beta\gamma' - \alpha''\beta'\gamma - \alpha\beta''\gamma' - \alpha'\beta\gamma''$$

debe ser $= +1$ o bien $= -1$. Le denotaremos por k. Observamos lo siguiente:

I. Si tenemos $\gamma = 0$, $\gamma' = 0$, $\alpha'' = 0$, $\beta'' = 0$, $\gamma'' = 1$ entonces

$$m = a\alpha^2 + 2b'\alpha\alpha' + a'\alpha'^2, \qquad m' = a\beta^2 + 2b''\beta\beta' + a'\beta'^2, \quad m'' = a''$$
$$n = b\beta' + b'\beta, \quad n' = b\alpha' + b'\alpha, \quad n'' = a\alpha\beta + b''(\alpha\beta' + \beta\alpha') + a'\alpha'\beta'$$

Además $\alpha\beta' - \beta\alpha'$ debe ser $= +1$ o bien $= -1$. Por tanto, es evidente que la forma binaria (a, b'', a'), cuyo determinante es A'', será transformada por medio de la sustitución α, β, α', β' en la forma binaria (m, n'', m') de determinante M'' y, dado que $\alpha\beta' - \beta\alpha' = \pm 1$, ellas serán equivalentes y, por ende, $M'' = A''$. Esto también puede ser confirmado directamente. A menos que, por esta razón, (a, b'', a') ya sea la forma más simple en esta clase, podemos determinar α, β, α', β' de tal manera que (m, n'', m') sea una forma más simple. A partir de la teoría de la equivalencia de formas binarias, es fácil concluir que esto puede hacerse de tal modo que m no sea mayor que $\sqrt{-\frac{4}{3}A''}$ si A'' es negativo, o bien, no mayor que $\sqrt{A''}$ cuando A'' es positivo o de tal manera que $m = 0$ cuando $A'' = 0$. Por ello, en todos los casos el valor (absoluto) de m puede hacerse menor o igual a $\sqrt{\pm\frac{4}{3}A''}$. De esta manera, la forma f es reducida a otra con un primer coeficiente menor, si esto es posible. Y la forma que es adjunta a ésta tiene el mismo tercer coeficiente que la forma F que es adjunta a f. Esta es la *primera reducción.*

II. Pero si $\alpha = 1$, $\beta = 0$, $\gamma = 0$, $\alpha' = 0$, $\alpha'' = 0$, resulta $k = \beta'\gamma'' - \beta''\gamma' = \pm 1$; así que la sustitución que es adjunta a S será

$$\begin{array}{rrr} \pm 1, & 0, & 0 \\ 0, & \gamma'', & -\beta'' \\ 0, & -\gamma', & \beta' \end{array}$$

y por esta sustitución F será transformada en G y tendremos

$$\begin{aligned} m =& a, \quad n' = b'\gamma'' + b''\gamma', \quad n'' = b'\beta'' + b''\beta' \\ m' =& a'\beta'^2 + 2b\beta'\beta'' + a''\beta''^2 \\ m'' =& a'\gamma'^2 + 2b\gamma'\gamma'' + a''\gamma''^2 \\ n =& a'\beta'\gamma' + b(\beta'\gamma'' + \gamma'\beta'') + a''\beta''\gamma'' \\ M' =& A'\gamma''^2 - 2B\gamma'\gamma'' + A''\gamma'^2 \\ N =& - A'\beta''\gamma'' + B(\beta'\gamma'' + \gamma'\beta'') - A''\beta'\gamma' \\ M'' =& A'\beta''^2 - 2B\beta'\beta'' + A''\beta'^2 \end{aligned}$$

De este modo, es claro que la forma binaria (A'', B, A'), cuyo determinante es Da, será transformada por medio de la sustitución β', $-\gamma'$, $-\beta''$, γ'' en la forma (M'', N, M') de determinante Dm, y por tanto (dado que $\beta'\gamma'' - \gamma'\beta'' = \pm 1$, o bien, dado que $Da = Dm$) es equivalente a ella. A menos que, por esta razón, (A'', B, A') ya sea la forma más simple de su clase, los coeficientes β', γ', β'', γ'' pueden ser determinados de tal manera que (M'', N, M') es más simple. Y esto puede lograrse de tal modo que, sin distingo de signo, M'' no es mayor que $\sqrt{\pm\frac{4}{3}Da}$. De este manera, la forma f es reducida a otra con el mismo primer coeficiente. Pero la forma que es adjunta a ésta tendrá, si es posible, un menor tercer coeficiente que la forma F, la cual es adjunta a f. Esta es la *segunda reducción.*

III. Ahora bien, si ni la primera ni la segunda reducción es aplicable a la forma ternaria f, es decir, si f no puede ser transformada por ninguna de ellas hacia una forma más simple; entonces necesariamente a^2 será $< \text{o} = \frac{4}{3}A''$, y A''^2 será, o bien $< \text{o} = \frac{4}{3}aD$, sin distingo de signo. Así, a^4 será $< \text{o} = \frac{16}{9}A''^2$, de modo que a^4 será $< \text{o} = \frac{64}{27}aD$, $a^3 < \text{o} = \frac{64}{27}D$, y $a < \text{o} = \frac{4}{3}\sqrt[3]{D}$; y, de nuevo, A''^2 será $< \text{o} = \frac{16}{9}\sqrt[3]{D^4}$ y $A'' < \text{o} = \frac{4}{3}\sqrt[3]{D^2}$. De ahí que, toda vez que a o A'' exceda estos límites, una u otra de las reducciones previas necesariamente se aplica a la forma f. Pero esta conclusión no puede ser invertida, dado que a menudo ocurre que el primer

coeficiente y el tercer coeficiente de la forma adjunta de una forma ternaria están ya por debajo de esos límites; sin embargo puede hacerse más simple por una u otra de las reducciones.

IV. Si ahora aplicamos alternativamente la primera y segunda reducción a una forma ternaria dada de determinante D, es decir, si aplicamos la primera o la segunda, entonces al resultado le aplicamos la segunda o la primera, y al resultado de esto de nuevo la primera o la segunda, etc., es claro que eventualmente arribaremos a una forma a la cual ninguna puede ser aplicada. Pues la magnitud absoluta de los primeros coeficientes de las formas en sí, y de los terceros coeficientes de las formas adjuntas se mantienen igual y luego decrecen de modo que la progresión eventualmente parará; de otro modo, tendríamos dos series infinitas de números continuamente decrecientes. Tenemos por tanto este notable teorema: *Cualquier forma ternaria de determinante D puede ser reducida a una forma equivalente con la propiedad de que su primer coeficiente no sea mayor que* $\frac{4}{3}\sqrt[3]{D}$ *y que el tercer coeficiente de la forma adjunta no sea mayor que* $\frac{4}{3}\sqrt[3]{D^2}$*, sin distinción de signo, siempre y cuando la forma propuesta no tenga ya estas propiedades.* En lugar del primer coeficiente de la forma f y del tercer coeficiente de la forma adjunta, podríamos haber considerado exactamente de la misma manera o el primer coeficiente de la forma y el segundo de su adjunta; o el segundo de la forma y el primero o tercero de su adjunta; o el tercero de la forma y el primero o segundo de su adjunta. Eventualmente llegaremos a la misma conclusión; pero es más ventajoso usar un método consistente de modo que las operaciones involucradas pueden ser reducidas hacia un algoritmo fijo. Observamos finalmente que si hubiéramos separado las formas en definidas e indefinidas, habríamos fijado límites inferiores para los dos coeficientes que hemos estado tratando; pero esto no es necesario para nuestros propósitos.

273.

Estos ejemplos ilustran los principios previos.

Ejemplo 1. Sea $f = \begin{pmatrix} 19, & 21, & 50 \\ 15, & 28, & 1 \end{pmatrix}$, luego $F = \begin{pmatrix} -825, & -166, & -398 \\ 257, & 573, & -370 \end{pmatrix}$ y $D = -1$. Dado que $(19, 1, 21)$ es una forma binaria reducida y no hay otra equivalente a ella que tenga su primer término menor que 19, la primera reducción no es aplicable aquí; la forma binaria $(A'', B, A') = (-398, 257, -166)$, por la teoría de la equivalencia de formas binarias, puede ser transformada en una equivalente más simple $(-2, 1, 10)$ por medio de la sustitución $2, 7, 3, 11$. Entonces, haciendo

$\beta' = 2$, $\gamma' = -7$, $\beta'' = -3$, $\gamma'' = 11$ y aplicando la sustitución

$$\left\{\begin{matrix} 1, & 0, & 0 \\ 0, & 2, & -7 \\ 0, & -3, & 11 \end{matrix}\right\}$$

a la forma f, ésta será transformada en $\begin{pmatrix} 19, & 354, & 4769 \\ -1299, & 301, & -82 \end{pmatrix} \dots f'$. El tercer coeficiente de la forma adjunta es -2, y en este aspecto, f' es más simple que f.

La primera reducción puede ser aplicada a la forma f'. Esto es, dado que la forma binaria $(19, -82, 354)$ es transformada en $(1, 0, 2)$ por medio de la sustitución 13, 4, 3, 1, la sustitución

$$\left\{\begin{matrix} 13, & 4, & 0 \\ 3, & 1, & 0 \\ 0, & 0, & 1 \end{matrix}\right\}$$

puede ser aplicada a la forma f' y será transformada en $\begin{pmatrix} 1, & 2, & 4769 \\ -95, & 16, & 0 \end{pmatrix} \dots f''$.

Puede aplicarse nuevamente la segunda reducción a la forma f'', cuya adjunta es $\begin{pmatrix} -513, & -4513, & -2 \\ -95, & 32, & 1520 \end{pmatrix}$. Esto es $(-2, -95, -4513)$ será transformada en $(-1, 1, -2)$ por medio de la sustitución 47, 1, -1, 0; así que la sustitución

$$\left\{\begin{matrix} 1, & 0, & 0 \\ 0, & 47, & -1 \\ 0, & 1, & 0 \end{matrix}\right\}$$

puede ser aplicada a f'' y será transformada en $\begin{pmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{pmatrix} \dots f'''$. El primer coeficiente de esta forma no puede ser reducido más de esto por medio de la primera reducción, ni puede ser el tercer coeficiente de la adjunta reducido más por medio de la segunda reducción.

Ejemplo 2. Sea $f = \begin{pmatrix} 10, & 26, & 2 \\ 7, & 0, & 4 \end{pmatrix}$, cuya adjunta es $\begin{pmatrix} -3, & -20, & -244 \\ 70, & -28, & 8 \end{pmatrix}$ y cuyo determinante es $= 2$. Aplicando alternativamente la segunda y la primera

reducción

por la sustitución	transformamos a	en
$\left\{\begin{matrix}1, & 0, & 0\\ 0, & -1, & 0\\ 0, & 4, & -1\end{matrix}\right\}$	f	$\left(\begin{matrix}10, & 2, & 2\\ -1, & 0, & -4\end{matrix}\right) = f'$
$\left\{\begin{matrix}0, & -1, & 0\\ 1, & -2, & 0\\ 0, & 0, & 1\end{matrix}\right\}$	f'	$\left(\begin{matrix}2, & 2, & 2\\ 2, & -1, & 0\end{matrix}\right) = f''$
$\left\{\begin{matrix}1, & 0, & 0\\ 0, & -1, & 0\\ 0, & 2, & -1\end{matrix}\right\}$	f''	$\left(\begin{matrix}2, & 2, & 2\\ -2, & 1, & -2\end{matrix}\right) = f'''$
$\left\{\begin{matrix}1, & 0, & 0\\ 1, & 1, & 0\\ 0, & 0, & 1\end{matrix}\right\}$	f'''	$\left(\begin{matrix}0, & 2, & 2\\ -2, & -1, & 0\end{matrix}\right) = f''''$

La forma f'''' no puede ser reducida más por medio de la primera o de la segunda reducción.

274.

Cuando se trata de una forma ternaria, donde su primer coeficiente y el tercer coeficiente de la forma adjunta han sido reducidos lo más posible por medio de los métodos precedentes, el siguiente método suministrará una reducción adicional.

Usando la misma notación que en el artículo 272 y haciendo $\alpha = 1$, $\alpha' = 0$, $\beta' = 1$, $\alpha'' = 0$, $\beta'' = 0$, $\gamma'' = 1$, a saber, usando la sustitución

$$\begin{matrix}1, & \beta, & \gamma\\ 0, & 1, & \gamma'\\ 0, & 0, & 1\end{matrix}$$

tendremos

$$m = a, \quad m' = a' + 2b''\beta + a\beta^2, \quad m'' = a'' + 2b\gamma' + 2b'\gamma + a\gamma^2 + 2b''\gamma\gamma' + a'\gamma'^2$$
$$n = b + a'\gamma' + b'\beta + b''(\gamma + \beta\gamma') + a\beta\gamma, \quad n' = b' + a\gamma + b''\gamma', \quad n'' = b'' + a\beta$$

y luego

$$M'' = A'', \quad N = B - A''\gamma', \quad N' = B' - N\beta - A''\gamma.$$

Tal transformación no cambia los coeficientes a y A'', los cuales fueron disminuidos por las reducciones anteriores. Resta, por tanto, encontrar una determinación adecuada de β, γ y γ' de tal modo que los coeficientes restantes sean disminuidos. Observamos primero que si $A'' = 0$ podemos suponer también que $a = 0$, pues si a no fuera $= 0$, la primera reducción sería aplicable una vez más, dado que cualquier forma binaria de determinante 0 es equivalente a una forma como $(0,\ 0,\ h)$ y su primer término es $= 0$ (véase art. 215). Por una razón completamente similar, es legítimo suponer que A'' también sería $= 0$ si $a = 0$, y por tanto, ya sea, ambos o ninguno de los números a y A'' serán 0.

En el segundo caso, β, γ y γ' pueden ser determinados de tal modo que, sin distinción de signo, n'', N, N' no son mayores que $\frac{1}{2}a$, $\frac{1}{2}A''$, $\frac{1}{2}A''$ respectivamente. De manera que en el primer ejemplo del artículo previo la última forma $\begin{pmatrix} 1, & 257, & 2 \\ 1, & 0, & 16 \end{pmatrix}$, cuya adjunta es $\begin{pmatrix} -513, & -2, & -1 \\ 1, & -16, & 32 \end{pmatrix}$ será transformada por medio de la sustitución

$$\begin{Bmatrix} 1, & -16, & 16 \\ 0, & 1, & -1 \\ 0, & 0, & 1 \end{Bmatrix}$$

en la forma $\begin{pmatrix} 1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix} \ldots f''''$, cuya adjunta es $\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$.

En el caso donde $a = A'' = 0$ y, por tanto, también $b'' = 0$ tendremos

$$m = 0, \quad m' = a', \quad m'' = a'' + 2b\gamma' + 2b'\gamma + a'\gamma'^2$$
$$n = b + a'\gamma' + b'\beta, \quad n' = b', \quad n'' = 0$$

y luego

$$D = a'b'^2 = m'n'^2$$

Es fácil ver que β y γ' pueden ser determinados de tal manera que n será igual al residuo absolutamente mínimo de b relativo al módulo que sea el máximo común divisor de a' y b'; a saber, de tal modo que n no sea mayor que la mitad de su divisor, sin considerar el signo, y n será 0 toda vez que a' y b' sean relativamente primos. Si β y γ' son determinados de esta manera, el valor de γ puede ser tomado tal que m'' no sea mayor que b' sin importar el signo. Esto, por supuesto, sería imposible si $b' = 0$, pero entonces D sería 0, el cual es el caso excluido. Así que para la última forma en

el segundo ejemplo del artículo previo, $n = -2-\beta+2\gamma'$, y poniendo $\beta = -2$, $\gamma' = 0$, tendremos $n = 0$; más aún $m'' = 2 - 2\gamma$, y poniendo $\gamma = 1$ entonces $m'' = 0$. Así tenemos la sustitución

$$\left\{\begin{matrix} 1, & -2, & 1 \\ 0, & 1, & 0 \\ 0, & 0, & 1 \end{matrix}\right\}$$

mediante la cual aquella forma será transformada en $\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix} \ldots f''''''$.

275.

Si se tiene una serie de formas ternarias equivalentes f, f', f'', f''', etc. y las transformaciones de cada una de estas formas en su sucesor: entonces, a partir de la transformación de la forma f en f' y de la forma f' en f'', por el artículo 270 podemos deducir una transformación de la forma f en f''; a partir de esto y de la transformación de la forma f'' en f''' resultará una transformación de la forma f en f''', etc. y por medio de este proceso se puede encontrar la transformación de la forma f en cualquier otra forma de la serie. Y dado que, a partir de la transformación de la forma f en cualquier otra forma equivalente g se puede deducir una transformación de la forma g en f (S'' a partir de S, art. 268, 269), se puede, de esta manera, producir una transformación de cualquiera de la serie f', f'', etc. en la primera forma f. Así para las formas del primer ejemplo del artículo previo encontramos las sustituciones

$$\begin{array}{rrr|rrr|rrr} 13, & 4, & 0 & 13, & 188, & -4 & 13, & -20, & 16 \\ 6, & 2, & -7 & 6, & 87, & -2 & 6, & -9, & 7 \\ -9, & -3, & 11 & -9, & -130, & 3 & -9, & 14, & -11 \end{array}$$

por medio de la cual f será transformada en f'', f''', f'''' respectivamente y, a partir de la última sustitución, podemos derivar

$$\left\{\begin{matrix} 1, & 4, & 4 \\ 3, & 1, & 5 \\ 3, & -2, & 3 \end{matrix}\right\}$$

mediante la cual f''' se transformará en f. Similarmente, tenemos las siguientes sustituciones para el ejemplo 2 del artículo anterior.

$$\begin{array}{rrr|rrr} 1, & -1, & 1 & 2, & -3, & -1 \\ -3, & 4, & -3 & 3, & 1, & 0 \\ 10, & -14, & 11 & 2, & 4, & 1 \end{array}$$

mediante las cuales la forma $\left(\begin{smallmatrix}10, 26, 2\\ 7, \ 0, 4\end{smallmatrix}\right)$ se transforma en $\left(\begin{smallmatrix}0, \ \ 2, 0\\ 0, -1, 0\end{smallmatrix}\right)$ y vice versa.

276.

TEOREMA. *El número de clases entre las cuales se distribuyen todas las formas ternarias de un determinante dado es siempre finito.*

Demostración. I. El número de todas las formas $\left(\begin{smallmatrix}a, a', a''\\ b, b', b''\end{smallmatrix}\right)$ de un determinante dado D en las cuales $a = 0$, $b'' = 0$, b no es mayor que la mitad del valor del máximo común divisor de a' y b', y a'' no es mayor que b', es obviamente finito. Pues, como debemos tener $a'b'^2 = D$, los únicos valores posibles de b' son $+1$, -1, y las raíces de cuadrados que son divisores de D (si hay otros diferentes de 1) tomadas positiva y negativamente. El número de ellos es finito. Para cada uno de los valores de b', sin embargo, el valor de a' es dado, y por lo tanto el número de valores de b y de a'' es finito.

II. Suponga que a no es $= 0$ ni mayor que $\frac{4}{3}\sqrt[3]{\pm D}$; que $b''^2 - aa' = A''$ y que no es $= 0$ ni mayor que $\frac{4}{3}\sqrt[3]{D^2}$; que b'' no es mayor que $\frac{1}{2}a$; que $ab - b'b'' = B$ y $a'b' - bb'' = B'$ y que ninguno es mayor que $\frac{1}{2}A''$. En este caso un argumento similar al anterior muestra que el número de todas las formas $\left(\begin{smallmatrix}a, a', a''\\ b, b', b''\end{smallmatrix}\right)$ de determinante D es finito. Pues el número de todas las combinaciones de los valores de a, b'', A'', B y B' será finito, y cuando se han determinado, los coeficientes restantes de la forma, a saber, a', b, b', a'' y los coeficientes de la forma adjunta

$$b^2 - a'a'' = A, \quad b'^2 - aa'' = A', \quad a''b'' - bb' = B''$$

estarán determinados por las siguientes ecuaciones:

$$a' = \frac{b''^2 - A''}{a}, \quad A' = \frac{B^2 - aD}{A''}, \quad A = \frac{B'^2 - a'D}{A''}, \quad B'' = \frac{BB' + b''D}{A''}$$

$$b = \frac{AB - B'B''}{D} = -\frac{Ba' + B'b''}{A''}, \quad b' = \frac{A'B' - BB''}{D} = -\frac{Bb'' + B'a}{A''}$$

$$a'' = \frac{b'^2 - A'}{a} = \frac{b^2 - A}{a'} = \frac{bb' + B''}{b''}$$

Ahora, cuando se han obtenido todas las formas, si escogemos de todas las combinaciones, los valores de a, b'', A'', B y B' que hacen que a', a'', b y b'' sean enteros, habrá un número finito de ellos.

III. Por lo tanto, todas las formas en I y II constituyen un número finito de clases, y si algunas formas son equivalentes resultarán menos clases que formas. Por las investigaciones anteriores, cualquier forma ternaria de determinante D es necesariamente equivalente a alguna de estas formas, i.e., pertenece a alguna de las clases definidas por éstas, o sea, estas clases incluirán todas las formas de determinante D, i.e., todas las formas ternarias de determinante D estarán distribuidas entre un número finito de clases. *Q. E. D.*

277.

Las reglas para generar todas las formas en I y II del artículo anterior siguen en forma natural de su definición; por lo tanto basta con dar algunos ejemplos. Para $D = 1$, las reglas I generan las siguientes seis (tomando uno de los signos dobles a la vez):

$$\begin{pmatrix} 0, & 1, 0 \\ 0, \pm 1, & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0, & 1, \pm 1 \\ 0, \pm 1, & 0 \end{pmatrix}$$

Para las formas II, a y A'' pueden asumir únicamente los valores $+1$ y -1, y por lo tanto para cada una de las combinaciones resultantes b'', B y B' deben ser $= 0$ y obtenemos las formas

$$\begin{pmatrix} 1, -1, 1 \\ 0, & 0, 0 \end{pmatrix}, \quad \begin{pmatrix} -1, 1, 1 \\ 0, 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, 1, -1 \\ 0, 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, -1, -1 \\ 0, & 0, & 0 \end{pmatrix}$$

Similarmente para $D = -1$ obtenemos seis formas I y cuatro formas II:

$$\begin{pmatrix} 0, -1, 0 \\ 0, \pm 1, 0 \end{pmatrix}, \quad \begin{pmatrix} 0, -1, \pm 1 \\ 0, \pm 1, & 0 \end{pmatrix};$$

$$\begin{pmatrix} 1, -1, -1 \\ 0, & 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, 1, -1 \\ 0, 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, -1, 1 \\ 0, & 0, 0 \end{pmatrix}, \quad \begin{pmatrix} 1, 1, 1 \\ 0, 0, 0 \end{pmatrix}$$

Para $D = 2$ tenemos las seis formas I:

$$\begin{pmatrix} 0, & 2, 0 \\ 0, \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 2, \pm 1 \\ 0, \pm 1, & 0 \end{pmatrix}$$

y las ocho formas II:

$$\begin{pmatrix} 1, -1, 2 \\ 0, & 0, 0 \end{pmatrix}, \quad \begin{pmatrix} -1, 1, 2 \\ 0, 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, 1, -2 \\ 0, 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, -1, -2 \\ 0, & 0, & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1, -2, 1 \\ 0, & 0, 0 \end{pmatrix}, \quad \begin{pmatrix} -1, 2, 1 \\ 0, 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, 2, -1 \\ 0, 0, & 0 \end{pmatrix}, \quad \begin{pmatrix} -1, -2, -1 \\ 0, & 0, & 0 \end{pmatrix}$$

Pero el número de clases de formas en estos tres casos es mucho menor que el número de formas. Es fácil confirmar que

I. La forma $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$ se transforma en

$$\begin{pmatrix} 0, & 1, & 0 \\ 0, & -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, & 1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1, & -1 \\ 0, & \pm 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$$

respectivamente mediante las sustituciones

$$\begin{array}{c|c|c|c} 1, 0, 0 \\ 0, 1, 0 \\ 0, 0, -1 & 0, 0, 1 \\ 0, 1, -1 \\ \pm 1, 1, 0 & 0, 0, 1 \\ 0, 1, 1 \\ \pm 1, -1, -1 & 1, 0, -1 \\ 1, 1, -1 \\ 0, -1, 1 \end{array}$$

y que la forma $\begin{pmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$ se transforma en $\begin{pmatrix} 1, & -1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$ y $\begin{pmatrix} -1, & 1, & 1 \\ 0, & 0, & 0 \end{pmatrix}$ por una permutación simple de las incógnitas. Entonces, las diez formas ternarias del determinante 1 se reducen a estas dos: $\begin{pmatrix} 0, & 1, & 0 \\ 0, & 1, & 0 \end{pmatrix}$, $\begin{pmatrix} -1, & -1, & -1 \\ 0, & 0, & 0 \end{pmatrix}$; para la primera, si lo prefiere, se puede tomar $\begin{pmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{pmatrix}$. Y puesto que la primera forma es indefinida y la segunda definida, es claro que cualquier forma ternaria indefinida de determinante 1 es equivalente a la forma $x^2 + 2yz$ y cualquier forma definida es equivalente a $-x^2 - y^2 - z^2$.

II. De manera similar encontramos que cualquier forma ternaria indefinida de determinante -1 es equivalente a la forma $-x^2 + 2yz$ y cualquier forma definida a $x^2 + y^2 + z^2$.

III. Para el determinante 2, la segunda, sexta y sétima de las ocho formas (II) pueden rechazarse inmediatamente porque pueden obtenerse a partir de la primera por una permutación simple de las incógnitas. Similarmente, la quinta se puede obtener a partir de la tercera y la octava a partir de la cuarta. Las tres formas restantes, junto con las seis formas I generarán tres clases; es decir $\begin{pmatrix} 0, & 2, & 0 \\ 0, & 1, & 0 \end{pmatrix}$ se transformará en $\begin{pmatrix} 0, & 2, & 0 \\ 0, & -1, & 0 \end{pmatrix}$ mediante la sustitución

$$\left\{ \begin{matrix} 1, & 0, & 0 \\ 0, & 1, & 0 \\ 0, & 0, & -1 \end{matrix} \right\}$$

y la forma $\begin{pmatrix} 1, & 1, & -2 \\ 0, & 0, & 0 \end{pmatrix}$ se transforma en

$$\begin{pmatrix} 0, & 2, & 1 \\ 0, & 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 2, & 1 \\ 0, & -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 2, & -1 \\ 0, & 1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 0, & 2, & -1 \\ 0, & -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1, & -1, & 2 \\ 0, & 0, & 0 \end{pmatrix}$$

respectivamente mediante las sustituciones

1,0,1	1,0,−1	1,0, 0	1,0,0	1,0,0
1,2,0	1,2, 0	1,2,−1	1,2,1	0,1,2
1,1,0	1,1, 0	1,1,−1	1,1,1	0,1,1

Por lo tanto, cualquier forma ternaria de determinante 2 es reducible a una de las siguientes tres formas

$$\begin{pmatrix} 0, 2, 0 \\ 0, 1, 0 \end{pmatrix}, \quad \begin{pmatrix} 1, 1, -2 \\ 0, 0, \quad 0 \end{pmatrix}, \quad \begin{pmatrix} -1, -1, -2 \\ 0, \quad 0, \quad 0 \end{pmatrix}$$

y, si lo prefiere, $\left(\begin{smallmatrix} 2, 0, 0 \\ 1, 0, 0 \end{smallmatrix}\right)$ puede reemplazar la primera. Claramente cualquier forma ternaria definida será necesariamente equivalente a la tercera $-x^2 - y^2 - 2z^2$, puesto que las dos primeras son indefinidas. Y una forma indefinida será equivalente a la primera o segunda; a la primera, $2x^2 + 2yz$ si sus tres primeros coeficientes son todos pares (obviamente tal forma se transformará en una forma similar mediante cualquier sustitución y por lo tanto no puede ser equivalente a la segunda forma); a la segunda forma $x^2 + y^2 - 2z^2$, si sus tres primeros coeficientes no son todos pares, sino que uno, dos o todos son impares (pues la primera forma $2x^2 + 2yz$, no se puede transformar en ésta).

Según este argumento, pudimos haber predicho a priori en los ejemplos del artículo 273, 274 que la forma definida $\left(\begin{smallmatrix} 19, 21, 50 \\ 15, 28, \quad 1 \end{smallmatrix}\right)$ de determinante -1 se reduciría a $x^2 + y^2 + z^2$ y que la forma indefinida $\left(\begin{smallmatrix} 10, 26, 2 \\ 7, \quad 0, 4 \end{smallmatrix}\right)$ de determinante 2 se reduciría a $2x^2 - 2yz$ o (lo que es lo mismo) a $2x^2 + 2yz$.

278.

Si las incógnitas de una forma ternaria son x, x' y x'', la forma *representará* números dando valores determinados a x, x' y x'' y representará formas binarias mediante las sustituciones

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u$$

donde m, n, m', etc. son números a determinar y t y u las incógnitas de la forma binaria. Ahora, para completar la teoría de formas ternarias necesitamos una solución de los siguientes problemas. I. Encontrar todas las representaciones de un número

dado por una forma ternaria dada. II. Encontrar todas las representaciones de una forma binaria dada por una forma ternaria dada. III. Juzgar si dos formas ternarias dadas del mismo determinante son equivalentes, y si lo son, encontrar todas las transformaciones de una en la otra. IV. Juzgar si una forma ternaria dada implica otra forma ternaria dada de determinante mayor, y si lo hace, asignar toda transformación de la primera en la segunda. Puesto que estos problemas son más complicados que los problemas análogos para formas binarias, los trataremos con más detalle en otra ocasión. Por el momento, restringiremos nuestra investigación a mostrar cómo el primer problema puede reducirse al segundo y el segundo al tercero. Mostraremos cómo resolver el tercer problema para casos muy simples que son particularmente ilustrativos del teorema de formas binarias, y excluiremos el cuarto problema del todo.

279.

LEMA: *Dados tres enteros cualesquiera a, a' y a'' (no todos $= 0$), encontrar otros seis B, B', B'', C, C' y C'' tales que*

$$B'C'' - B''C' = a, \quad B''C - BC'' = a', \quad BC' - B'C = a''$$

Solución. Sea α el máximo común divisor de a, a' y a'' y escoja los enteros A, A' y A'' tales que

$$Aa + A'a' + A''a'' = \alpha$$

Ahora escoja arbitrariamente tres enteros $\mathfrak{C}$, $\mathfrak{C}'$ y $\mathfrak{C}''$ con la única restricción de que los tres números $\mathfrak{C}'A'' - \mathfrak{C}''A'$, $\mathfrak{C}''A - \mathfrak{C}A''$ y $\mathfrak{C}A' - \mathfrak{C}'A$ no son todos $= 0$. Designaremos estos números por b, b' y b'' respectivamente y su máximo común divisor por β. Entonces, si se pone

$$a'b'' - a''b' = \alpha\beta C, \quad a''b - ab'' = \alpha\beta C', \quad ab' - a'b = \alpha\beta C''$$

es claro que C, C' y C'' son enteros. Finalmente si escogemos enteros $\mathfrak{B}$, $\mathfrak{B}'$ y $\mathfrak{B}''$ tales que

$$\mathfrak{B}b + \mathfrak{B}'b' + \mathfrak{B}''b'' = \beta$$

poniendo

$$\mathfrak{B}a + \mathfrak{B}'a' + \mathfrak{B}''a'' = h$$

y fijando

$$B = \alpha\mathfrak{B} - hA, \quad B' = \alpha\mathfrak{B}' - hA', \quad B'' = \alpha\mathfrak{B}'' - hA''$$

los valores de B, B', B'', C, C' y C'' satisfarán las ecuaciones dadas.

En efecto, se encuentra que

$$aB + a'B' + a''B'' = 0$$
$$bA + b'A' + b''A'' = 0 \quad \text{y por lo tanto} \quad bB + b'B' + b''B'' = \alpha\beta$$

Ahora, a partir de los valores de C' y C'' tenemos

$$\begin{aligned}\alpha\beta(B'C'' - B''C') &= ab'B' - a'bB' - a''bB'' + ab''B'' \\ &= a(bB + b'B' + b''B'') - b(aB + a'B' + a''B'') = \alpha\beta a\end{aligned}$$

y así $B'C'' - B''C' = a$; similarmente encontramos que $B''C - BC'' = a'$ y $BC' - B'C = a''$. *Q. E. F.* Pero debemos omitir aquí el análisis mediante el cual encontramos esta solución y el método para encontrar todas las demás a partir de una de ellas.

280.

Supongamos que la forma binaria

$$at^2 + 2btu + cu^2 \ldots \varphi$$

cuyo determinante $= D$ es representada por la forma ternaria f con incógnitas x, x' y x'', poniendo

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u$$

y que la adjunta de f es la forma F con incógnitas X, X' y X''. Entonces, es fácil confirmar, mediante cálculos, (designando los coeficientes de f y F por letras) o por deducción a partir del artículo 268.II, que el número D es representable por F poniendo

$$X = m'n'' - m''n', \quad X' = m''n - mn'', \quad X'' = mn' - m'n$$

Se puede decir que esta representación del número D es la *adjunta* de la representación de la forma φ por f. Si los valores de X, X' y X'' no tienen un divisor común, para abreviar llamaremos *propia* esta representación de D, de otra manera, será *impropia* y también daremos estas mismas designaciones a la representación de la forma φ por f a la cual la representación de D es adjunta. Ahora, el descubrimiento de todas las representaciones propias del número D por la forma F se basa en las siguientes consideraciones:

I. No hay ninguna representación de D por la forma F que no se pueda deducir de alguna representación de una forma de determinante D por la forma f, i.e. que es adjunta a tal representación.

En efecto, sea $X = L$, $X' = L'$, $X'' = L''$ una representación cualquiera de D por F; por el lema del artículo anterior escoja m, m', m'', n, n' y n'' tales que

$$m'n'' - m''n' = L, \quad m''n - mn'' = L', \quad mn' - m'n = L''$$

y transforme f en la forma binaria $\varphi = at^2 + 2btu + cu^2$ por la sustitución

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u$$

Es fácil ver que D será el determinante de la forma φ y que la representación de D por F será la adjunta de la representación de φ por f.

Ejemplo. Sea $f = x^2 + x'^2 + x''^2$ y $F = -X^2 - X'^2 - X''^2$; $D = -209$; su representación por F será $X = 1$, $X' = 8$, $X'' = 12$; y encontramos que los valores de m, m', m'', n, n' y n'' son -20, 1, 1, -12, 0 y 1 respectivamente y $\varphi = 402t^2 + 482tu + 145u^2$.

II. Si φ y χ son formas binarias propiamente equivalentes, cualquier representación de D por F que es la adjunta de una representación de φ por f será también adjunta a una representación de la forma χ por f.

Sean p y q las incógnitas de la forma χ; transforme φ en χ mediante la sustitución propia $t = \alpha p + \beta q$, $u = \gamma p + \delta q$ y sea

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u \ldots (R)$$

alguna representación de la forma φ por f. Entonces si se pone

$$\begin{array}{lll} \alpha m + \gamma n = g, & \alpha m' + \gamma n' = g', & \alpha m'' + \gamma n'' = g'' \\ \beta m + \delta n = h, & \beta m' + \delta n' = h', & \beta m'' + \delta n'' = h'' \end{array}$$

la forma χ estará representada por f fijando

$$x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q \ldots (R')$$

y mediante cálculos (puesto que $\alpha\delta - \beta\gamma = 1$) encontramos

$$g'h'' - g''h' = m'n'' - m''n', \quad g''h - gh'' = m''n - mn'', \quad gh' - g'h = mn' - m'n$$

i.e. la misma representación de D por F es adjunta a las representaciones R y R'.

En el ejemplo anterior la forma φ es equivalente a $\chi = 13p^2 - 10pq + 18q^2$ y se transforma en ella mediante la sustitución propia $t = -3p + q$, $u = 5p - 2q$; y la representación de la forma χ por f es: $x = 4q$, $x' = -3p + q$, $x'' = 2p - q$. A partir de esto deducimos la misma representación del número -209 que teníamos antes.

III. Finalmente, si dos formas binarias φ y χ de determinante D cuyas incógnitas son t, u; p, q, se pueden representar por f y si la misma representación propia de D por F es adjunta a la representación de cada una de éstas, las dos formas deben ser propiamente equivalentes. Supongamos que φ se representa por f poniendo

$$x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u$$

y que χ se representa por f fijando

$$x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q$$

y que

$$m'n'' - m''n' = g'h'' - g''h' = L$$
$$m''n - mn'' = g''h - gh'' = L'$$
$$mn' - m'n = gh' - g'h = L''$$

Ahora escoja los enteros l, l' y l'' tales que $Ll + L'l' + L''l'' = 1$ y sea

$$n'l'' - n''l' = M, \quad n''l - nl'' = M', \quad nl' - n'l = M''$$
$$l'm'' - l''m' = N, \quad l''m - lm'' = N', \quad lm' - l'm = N''$$

y finalmente, sea

$$gM + g'M' + g''M'' = \alpha, \quad hM + h'M' + h''M'' = \beta$$
$$gN + g'N' + g''N'' = \gamma, \quad hN + h'N' + h''N'' = \delta$$

A partir de esto es fácil deducir

$$\alpha m + \gamma n = g - l(gL + g'L' + g''L'') = g$$
$$\beta m + \delta n = h - l(hL + h'L' + h''L'') = h$$

y similarmente

$$\alpha m' + \gamma n' = g', \quad \beta m' + \delta n' = h', \quad \alpha m'' + \gamma n'' = g'', \quad \beta m'' + \delta n'' = h''$$

A partir de esto es claro que $mt+nu$, $m't+n'u$, $m''t+n''u$ se transformará en $gp+hq$, $g'p + h'q$, $g''p + h''q$, respectivamente, mediante la sustitución

$$t = \alpha p + \beta q, \quad u = \gamma p + \delta q \ldots (S)$$

y mediante la sustitución S, φ se transformará en la misma forma que f poniendo

$$x = gp + hq, \quad x' = g'p + h'q, \quad x'' = g''p + h''q$$

es decir, en χ a la cual debe, por lo tanto, ser equivalente. Finalmente, mediante las sustituciones adecuadas se encuentra que

$$\alpha\delta - \beta\gamma = (Ll + L'l' + L''l'')^2 = 1$$

Por lo tanto, la sustitución S es propia y las formas φ y χ son propiamente equivalentes.

Como resultado de estas observaciones se derivan las siguientes reglas para encontrar toda representación propia de D por F: Encontrar todas las clases de formas binarias de determinante D y de ellas seleccionar una forma arbitraria; encontrar todas las representaciones propias de cada una de estas formas por f (desechando cualquiera que no se puede representar por f) y de cada una de estas representaciones, deducir representaciones del número D por F. Mediante I y II es claro que de esta manera se obtienen todas las representaciones propias posibles y que, por lo tanto, la solución es completa; mediante III es claro que transformaciones de formas de diferentes clases producen representaciones diferentes.

281.

La investigación de representaciones *impropias* de un número dado D por la forma F puede reducirse fácilmente al caso anterior. Es evidente que si D no es divisible por ningún cuadrado (excepto 1), no habrá ninguna representación de este tipo; pero si λ^2, μ^2, ν^2, etc. son divisores cuadrados de D, todas las representaciones impropias de D por F pueden encontrarse si primero encontramos todas las representaciones propias de los números $\frac{D}{\lambda^2}$, $\frac{D}{\mu^2}$, $\frac{D}{\nu^2}$, etc. por esta misma forma y se multiplican los valores de las incógnitas por λ, μ, ν, etc. respectivamente.

Por lo tanto, el poder encontrar todas las posibles representaciones de un número dado por una forma ternaria dada, *la cual es adjunta a otra forma ternaria*, depende del segundo problema. Y aunque a primera vista esto parece ser un caso muy particular, los demás casos se pueden reducir a éste como sigue. Sea D el número que se quiere representar por la forma $\left(\begin{smallmatrix} g, & g', & g'' \\ h, & h', & h'' \end{smallmatrix}\right)$ de determinante Δ, cuya adjunta es la forma $\left(\begin{smallmatrix} G, & G', & G'' \\ H, & H', & H'' \end{smallmatrix}\right) = f$. Entonces la adjunta de f será $\left(\begin{smallmatrix} \Delta g, & \Delta g', & \Delta g'' \\ \Delta h, & \Delta h', & \Delta h'' \end{smallmatrix}\right) = F$, y es claro que las representaciones del número ΔD por F (esta investigación depende de la anterior) serán idénticas a las representaciones del número D por la forma propuesta. Pero, cuando todos los coeficientes de la forma f tienen un divisor común μ, es evidente que todos los coeficientes de la forma F serán divisibles por μ^2 y así ΔD también debe ser divisible por μ^2 (de otra manera, no habrían representaciones); y representaciones del número D por la forma propuesta coincidirán con representaciones del número $\frac{\Delta D}{\mu^2}$ por la forma que resulta de dividir cada uno de los coeficientes de F por μ^2, y esta forma será adjunta a la forma que resulta de dividir cada coeficiente por μ.

Observamos, finalmente, que la solución del primer problema no es aplicable en el caso donde $D = 0$; pues en este caso, las formas binarias del determinante D no están distribuidas entre un número finito de clases; resolveremos posteriormente este caso, utilizando principios diferentes.

282.

La investigación de las representaciones de una forma binaria dada de determinante distinto de 0*) por una forma ternaria, depende de las siguientes

*) Para abreviar omitiremos un tratamiento del caso en el cual el determinante sea cero, puesto que requiere un método un poco distinto.

observaciones.

I. De cualquier representación propia de una forma binaria $(p, q, r) = \varphi$ de determinante D por la forma ternaria f de determinante Δ se pueden deducir enteros B y B' tales que

$$B^2 \equiv \Delta p, \qquad BB' \equiv -\Delta q, \qquad B'^2 \equiv \Delta r \pmod{D}$$

i.e. un valor de la expresión $\sqrt{\Delta(p, -q, r)} \pmod{D}$. Tómese la siguiente representación propia de la forma φ por f

$$x = \alpha t + \beta u, \qquad x' = \alpha' t + \beta' u, \qquad x'' = \alpha'' t + \beta'' u$$

(donde x, x' y x''; t y u designan las incógnitas de las formas f y φ); escoja enteros γ, γ' y γ'' tales que

$$(\alpha'\beta'' - \alpha''\beta')\gamma + (\alpha''\beta - \alpha\beta'')\gamma' + (\alpha\beta' - \alpha'\beta)\gamma'' = k$$

con $k = +1$ o $= -1$. Transforme f mediante la sustitución

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

en la forma $\left(\begin{smallmatrix} a, a', a'' \\ b, b', b'' \end{smallmatrix}\right) = g$, cuya adjunta es $\left(\begin{smallmatrix} A, A', A'' \\ B, B', B'' \end{smallmatrix}\right) = G$. Entonces, claramente resulta $a = p$, $b'' = q$, $a' = r$, $A'' = D$, y Δ el determinante de la forma g; por lo tanto

$$B^2 = \Delta p + A'D, \quad BB' = -\Delta q + B''D, \quad B'^2 = \Delta r + AD$$

Entonces, por ejemplo, la forma $19t^2 + 6tu + 41u^2$ es representada por $x^2 + x'^2 + x''^2$ poniendo $x = 3t + 5u$, $x' = 3t - 4u$, $x'' = t$; y fijando $\gamma = -1$, $\gamma' = 1$, $\gamma'' = 0$, tendremos $B = -171$, $B' = 27$ o sea $(-171, 27)$ como un valor de la expresión $\sqrt{-1(19, -3, 41)} \pmod{770}$.

Se sigue de esto que si $\Delta(p, -q, r)$ no es un residuo cuadrático de D, φ no podrá representarse propiamente por ninguna forma ternaria de determinante Δ; entonces, en el caso donde Δ y D son primos relativos, Δ tendrá que ser el número característico de la forma φ.

II. Puesto que γ, γ' y γ'' pueden determinarse de una infinidad de maneras diferentes, resultarán diferentes valores de B y B'. Veamos que relación tendrán entre sí. Suponga que también hemos escogido δ, δ' y δ'', tales que

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \mathfrak{k}$$

se hace $= +1$ o -1 y que la forma f se transforma mediante la sustitución

$$\begin{matrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{matrix}$$

en $\begin{pmatrix} \mathfrak{a}, \mathfrak{a}', \mathfrak{a}'' \\ \mathfrak{b}, \mathfrak{b}', \mathfrak{b}'' \end{pmatrix} = \mathfrak{g}$ con adjunta $\begin{pmatrix} \mathfrak{A}, \mathfrak{A}', \mathfrak{A}'' \\ \mathfrak{B}, \mathfrak{B}', \mathfrak{B}'' \end{pmatrix} = \mathfrak{G}$. Entonces g y $\mathfrak{g}$ serán equivalentes y así también G y $\mathfrak{G}$, y por una aplicación de los principios dados en los artículos 269 y 270*) encontraremos que si se fijan

$$(\beta'\gamma'' - \beta''\gamma')\delta + (\beta''\gamma - \beta\gamma'')\delta' + (\beta\gamma' - \beta'\gamma)\delta'' = \zeta$$
$$(\gamma'\alpha'' - \gamma''\alpha')\delta + (\gamma''\alpha - \gamma\alpha'')\delta' + (\gamma\alpha' - \gamma'\alpha)\delta'' = \eta$$

la forma $\mathfrak{G}$ se transformará en G mediante la sustitución

$$\begin{matrix} k, & 0, & 0 \\ 0, & k, & 0 \\ \zeta, & \eta, & \mathfrak{k} \end{matrix}$$

Entonces resulta

$$B = \eta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}, \quad B' = \zeta\mathfrak{k}D + \mathfrak{k}k\mathfrak{B}'$$

y así, puesto que $\mathfrak{k}k = \pm 1$, tendremos $B \equiv \mathfrak{B}$, $B' \equiv \mathfrak{B}'$ o $B \equiv -\mathfrak{B}$, $B' \equiv -\mathfrak{B}'$ (mod. D). En el primer caso diremos que los valores (B, B') y $(\mathfrak{B}, \mathfrak{B}')$ son equivalentes, en el segundo caso, que son opuestos; y diremos que las representaciones de la forma φ *pertenecen* a cualquiera de los valores de la expresión $\sqrt{\Delta(p, -q, r)}$ (mod. D) que puede deducirse mediante el método de I. Así pues, todos los valores a los cuales les corresponde la misma representación, serán equivalentes u opuestos.

*) Obtenemos la transformación de la forma g en la forma f a partir de la transformación de la forma f en la forma g; a partir de esto y de la transformación de la forma f en la forma $\mathfrak{g}$ obtenemos la transformación de la forma g en la forma $\mathfrak{g}$; y a partir de ésta, por transposición, la transformación de $\mathfrak{G}$ en G.

III. En cambio, como en I, si $x = \alpha t + \beta u$ etc. es una representación de la forma φ por f, y si esta representación pertenece al valor (B, B') del cual se deduce mediante la transformación

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

la misma representación también pertenecerá a cualquier otro valor $(\mathfrak{B}, \mathfrak{B}')$ que le es equivalente u opuesto; i.e., en lugar de γ, γ' y γ'' podemos tomar otros enteros δ, δ' y δ'' para los cuales la ecuación

$$(\alpha'\beta'' - \alpha''\beta')\delta + (\alpha''\beta - \alpha\beta'')\delta' + (\alpha\beta' - \alpha'\beta)\delta'' = \pm 1 \qquad (\Omega)$$

tiene lugar y se escogieran tales que, si f se transforma en su forma adjunta mediante la sustitución (S):

$$\begin{matrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{matrix}$$

el cuarto y quinto coeficiente de la forma adjunta serán respectivamente $= \mathfrak{B}$, $\mathfrak{B}'$. En efecto, sea

$$\pm B = \mathfrak{B} + \eta D, \quad \pm B' = \mathfrak{B}' + \zeta D$$

(aquí y más adelante tomaremos el signo superior e inferior según los valores de (B, B') y $(\mathfrak{B}, \mathfrak{B}')$ sean equivalentes u opuestos); ζ y η serán enteros y mediante la sustitución

$$\begin{matrix} 1, & 0, & \zeta \\ 0, & 1, & \eta \\ 0, & 0, & \pm 1 \end{matrix}$$

g se transformará en una forma $\mathfrak{g}$ con determinante Δ. Es fácil ver que los coeficientes 4 y 5 de la forma adjunta serán $= \mathfrak{B}$, $\mathfrak{B}'$ respectivamente. Sin embargo, si fijamos

$$\alpha\zeta + \beta\eta \pm \gamma = \delta, \quad \alpha'\zeta + \beta'\eta \pm \gamma' = \delta', \quad \alpha''\zeta + \beta''\eta \pm \gamma'' = \delta''$$

no es difícil ver que f se transformará en $\mathfrak{g}$ mediante la sustitución (S) y que la ecuación (Ω) será satisfecha. *Q. E. D.*

283.

A partir de estos principios se deduce el siguiente método para encontrar todas las representaciones propias de la forma binaria

$$\varphi = pt^2 + 2qtu + ru^2$$

de determinante D por la forma ternaria f de determinante Δ.

I. Se buscan todas los valores diferentes (i.e. no equivalentes) de la expresión $\sqrt{\Delta(p,-q,r)}$ (mod. D). Para el caso en el cual φ es una forma primitiva y Δ y D primos relativos, la solución fue dada en el art. 233, y los casos restantes se pueden reducir facilmente a éste. Para abreviar no daremos una explicación más completa. Simplemente indicaremos que siempre que Δ y D sean primos relativos, la expresión $\Delta(p,-q,r)$ no puede ser un residuo cuadrático de D a menos que φ sea una forma primitiva. En efecto, suponiendo

$$\Delta p = B^2 - DA', \quad -\Delta q = BB' - DB'', \quad \Delta r = B'^2 - DA$$

entonces

$$(DB'' - \Delta q)^2 = (DA' + \Delta p)(DA + \Delta r)$$

y manipulando y sustituyendo D por $q^2 - pr$ tenemos

$$(q^2 - pr)(B''^2 - AA') - \Delta(Ap + 2B''q + A'r) + \Delta^2 = 0$$

y es fácil concluir que si p, q y r, tienen un divisor común, también éste será un factor de Δ^2; por consiguiente Δ y D no podrían ser primos relativos. Por lo tanto p, q y r no pueden tener un divisor común y φ es una forma primitiva.

II. Designemos el número de estos valores por m y supongamos que entre ellos hay n que son opuestos a sí mismos (fijando $n = 0$ cuando no los hay). Entonces es claro que los restantes $m - n$ valores estarán compuestos por parejas que son opuestas entre sí (puesto que hemos supuesto que se incluyen todos los valores); ahora, si de cada par de valores opuestos rechazamos un valor arbitrariamente, nos quedarán $\frac{1}{2}(m+n)$ valores en total. Así pues por ejemplo, tenemos ocho valores de la expresión $\sqrt{-1(19,-3,41)}$ (mod. 770), a saber, $(39,237)$, $(171,-27)$, $(269,-83)$, $(291,-127)$, $(-39,-237)$, $(-171,27)$, $(-269,83)$ y $(-291,127)$. Rechazamos los cuatro últimos como opuestos a los primeros. Pero es evidente que si (B,B') es un valor que es opuesto a sí mismo, $2B$, $2B'$ y también $2\Delta p$, $2\Delta q$ y $2\Delta r$ serán divisibles por D; y

por lo tanto, si Δ y D son primos relativos, $2p$, $2q$ y $2r$, también serán divisibles por D. Según I, en este caso p, q y r no pueden tener un divisor común, entonces 2 debe ser divisible por D. Esto no puede ocurrir a menos que D sea $= \pm 1$ o $= \pm 2$. Así pues, para todos los valores de D mayores que 2, siempre resulta $n = 0$ si Δ y D son primos relativos.

III. Al ver esto, es evidente que cualquier representación propia de la forma φ por f debe pertenecer a uno y sólo uno de los valores restantes. Deberíamos, por lo tanto, revisar cada uno de estos valores en orden para encontrar la representación que pertenece a cada uno. Para poder encontrar la representación correspondiente a un valor *dado* (B, B') debemos determinar primero la forma ternaria $g = \left(\begin{smallmatrix} a, & a', & a'' \\ b, & b', & b'' \end{smallmatrix}\right)$ cuyo determinante $= \Delta$ y en la cual $a = p$, $b'' = q$, $a' = r$, $ab - b'b'' = B$, $a'b' - bb'' = B'$; los valores a'', b y b' se pueden encontrar con la ayuda de la ecuación del artículo 276.II. A partir de éstos es fácil ver que cuando Δ y D son primos relativos, b, b' y a'' deben ser enteros (puesto que estos tres números dan valores enteros cuando son multiplicados por D y luego por Δ). Ahora, si alguno de los coeficientes b, b' y a'' es una fracción o las formas f y g no son equivalentes, no habrá ninguna representación de la forma φ por f perteneciente a (B, B'); pero si b, b' y a'' son enteros y las formas f y g son equivalentes, entonces, cualquier transformación de f en g, por ejemplo

$$\begin{matrix} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{matrix}$$

producirá tal representación, a saber,

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u$$

Es claro que no puede existir ninguna representación de este tipo que no se pueda deducir de alguna transformación. Entonces aquella parte del segundo problema que se refiere a la representación *propia* se reduce al tercer problema.

IV. Ahora, transformaciones diferentes de la forma f en la forma g siempre producen representaciones distintas, con la única excepción del caso en el cual el valor (B, B') es opuesto a sí mismo. En este caso dos transformaciones dan una sola representación. En efecto, suponga que f también se transforma en g mediante la sustitución

$$\begin{matrix} \alpha, & \beta, & \delta \\ \alpha', & \beta', & \delta' \\ \alpha'', & \beta'', & \delta'' \end{matrix}$$

(que da la misma representación que la anterior) y sean k, $\mathfrak{k}$, ζ y η los mismos números que en II del artículo anterior. Tendremos

$$B = k\mathfrak{k}B + \eta\mathfrak{k}D, \quad B' = k\mathfrak{k}B' + \zeta\mathfrak{k}D$$

Si se supone que ambas k, $\mathfrak{k} = +1$ ó $= -1$, encontramos (ya que hemos excluido el caso de $D = 0$) que $\zeta = 0$, $\eta = 0$ y se sigue que $\delta = \gamma$, $\delta' = \gamma'$, $\delta'' = \gamma''$; estas dos transformaciones pueden ser diferentes sólo cuando uno de los números k o $\mathfrak{k}$ es $+1$ y el otro -1; entonces tenemos $B \equiv -B$, $B' \equiv -B'$ (mod. D) o el valor de (B, B') es opuesto a sí mismo.

V. A partir de lo dicho anteriormente (art. 271) sobre los criterios para formas definidas e indefinidas, se sigue fácilmente que si Δ es positivo, D es negativo, y φ es una forma negativa, g será una forma negativa definida, pero si Δ es positivo y D es positivo (o bien D es negativo y φ una forma positiva), g será una forma indefinida. Ahora, puesto que f y g definitivamente no pueden ser equivalentes, a menos que sean similares en cuanto a esto, es claro que formas binarias con determinantes positivos y formas positivas no pueden ser representadas propiamente por una forma ternaria negativa, y que formas binarias negativas no pueden representarse por formas ternarias indefinidas con determinante positivo; pero una forma ternaria del primer tipo puede representar una forma del segundo tipo, y una forma ternaria del segundo tipo puede representar una forma del primer tipo únicamente. Similarmente, concluimos que una forma ternaria definida (i.e. positiva) con determinante negativo puede representar únicamente formas binarias positivas, y que una forma ternaria indefinida con determinante negativo solamente puede representar formas binarias negativas y formas con determinante positivo.

284.

Representaciones *impropias* de la forma binaria φ con determinante D por la forma ternaria f, cuya adjunta es F, son aquéllas de las cuales deducimos representaciones impropias del número D por la forma F. Por lo tanto, es claro que φ no se puede representar impropiamente por f a menos que D tenga factores cuadrados. Supongamos que todos los cuadrados (excepto 1) que son divisores de D son e^2, e'^2, e''^2, etc. (el número de ellos es finito ya que hemos excluido la posibilidad de tener $D = 0$). Toda representación impropia de la forma φ por f dará una representación del número D por F, en la cual los valores de las incógnitas tendrán

alguno de los números e, e', e'', etc. como máximo común divisor. Por esta razón decimos simplemente que una representación impropia de la forma φ *pertenece* al divisor cuadrado e^2, o e'^2, o e''^2, etc. Ahora se utilizan las reglas siguientes para encontrar todas las representaciones de la forma φ que pertenecen al mismo divisor *dado* e^2 (supondremos que su raíz cuadrada e se toma positivamente). Para abreviar daremos una demostración sintética, pero será fácil reconstruir el análisis que produce los resultados.

Primero encuentre todas la formas binarias de determinante $\frac{D}{e^2}$ que se transforman en φ mediante una sustitución propia como $T = \chi t + \lambda u$, $U = \mu u$, donde T y U son incógnitas de tal forma; t y u incógnitas de la forma φ; χ y μ enteros positivos (cuyo producto es por lo tanto $= e$); λ un entero positivo menor que μ (puede ser cero). Estas formas, con las transformaciones correspondientes, se pueden encontrar como sigue.

Sea χ igual, sucesivamente, a cada uno de los divisores de e tomados positivamente (incluyendo a 1 y a e) y sea $\mu = \frac{e}{\chi}$; para cada uno de los valores enteros χ y μ, asigne a λ todos los valores enteros desde cero hasta $\mu - 1$, y de seguro tendremos todas las transformaciones. Ahora podemos encontrar la forma que se transforma en φ mediante una sustitución $T = \chi t + \lambda u$, $U = \mu u$, investigando la forma en la cual se transforma φ mediante la sustitución $t = \frac{1}{\chi}T - \frac{\lambda}{e}U$, $u = \frac{1}{\mu}U$; así se obtendrán las formas correspondientes a cada una de las transformaciones; pero sólo aquellas formas en las cuales los tres coeficientes son enteros*) deben ser retenidas.

Segundo, supongamos que Φ es una de las formas que se transforma en φ mediante la sustitución $T = \chi t + \lambda u$, $U = \mu u$; se investigan todas las representaciones *propias* de la forma Φ por f (si existe alguna) y se exhiben en general por la fórmula:

$$x = \mathfrak{A}T + \mathfrak{B}U, \quad x' = \mathfrak{A}'T + \mathfrak{B}'U, \quad x'' = \mathfrak{A}''T + \mathfrak{B}''U \qquad (\mathfrak{R})$$

De cada uno de los $(\mathfrak{R})$ se deduce una representación

$$x = \alpha t + \beta u, \quad x' = \alpha' t + \beta' u, \quad x'' = \alpha'' t + \beta'' u \qquad (\rho)$$

*) Si pudiéramos tratar más ampliamente este problema, podríamos abreviar, en gran medida, la solución. Es inmediatamente obvio que para χ necesitamos considerar solamente aquellos divisores de e cuyos cuadrados dividen el primer coeficiente de la forma φ. Reservaremos para una ocasión más apropiada un estudio más profundo de éste problema. Note que podemos deducir de él soluciones más sencillas de los problemas de los artículos 213 y 214.

mediante las ecuaciones

$$\begin{array}{lll} \alpha = \chi\mathfrak{A}, & \alpha' = \chi\mathfrak{A}', & \alpha'' = \chi\mathfrak{A}'' \\ \beta = \lambda\mathfrak{A} + \mu\mathfrak{B}, & \beta' = \lambda\mathfrak{A}' + \mu\mathfrak{B}', & \beta'' = \lambda\mathfrak{A}'' + \mu\mathfrak{B}'' \end{array} \qquad (R)$$

Al tratar de la misma manera todas las otras formas que encontramos mediante la primera regla (si hay varias), otras representaciones serán obtenidas a partir de cada representación propia de cada forma. De esta manera obtendremos todas las representaciones de la forma φ que pertenecen al divisor e^2 y cada una sólo una vez.

Demostración. I. Es tan obvio que la forma ternaria f se transforma en φ por cada sustitución (ρ) que no necesita de una explicación adicional; que cada representación (ρ) es impropia y pertenece al divisor e^2 es claro en vista de que los números $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$, $\alpha\beta' - \alpha'\beta$ son $= e(\mathfrak{A}'\mathfrak{B}'' - \mathfrak{A}''\mathfrak{B}')$, $e(\mathfrak{A}''\mathfrak{B} - \mathfrak{A}\mathfrak{B}'')$, $e(\mathfrak{A}\mathfrak{B}' - \mathfrak{A}'\mathfrak{B})$ respectivamente y su máximo común divisor será e (puesto que $(\mathfrak{R})$ es una representación propia).

II. Mostraremos que a partir de cualquier representación (ρ) de la forma φ se puede encontrar una representación propia de una forma de determinante $\frac{D}{e^2}$ contenida entre las formas encontradas mediante la primera regla; eso es, a partir de los valores dados α, α', α'', β, β' y β'' podemos deducir valores enteros χ, λ y μ con las condiciones prescritas, tanto como los valores de $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$, $\mathfrak{B}$, $\mathfrak{B}'$ y $\mathfrak{B}''$ que satisfacen unívocamente a las ecuaciones (R). Es inmediatamente claro de las tres primeras ecuaciones de (R) que para χ debemos tomar el máximo común divisor de α, α' y α'' con signo positivo (ya que $\mathfrak{A}'\mathfrak{B}'' - \mathfrak{A}''\mathfrak{B}'$, $\mathfrak{A}''\mathfrak{B} - \mathfrak{A}B''$ y $\mathfrak{A}\mathfrak{B}' - \mathfrak{A}'\mathfrak{B}$ no tienen un divisor común, y $\mathfrak{A}$, $\mathfrak{A}'$ y $\mathfrak{A}''$ tampoco); por lo tanto están determinados $\mathfrak{A}$, $\mathfrak{A}'$, $\mathfrak{A}''$ y $\mu = \frac{e}{\chi}$ (es fácil ver que necesariamente serán enteros). Supongamos que los tres enteros $\mathfrak{a}$, $\mathfrak{a}'$ y $\mathfrak{a}''$ hacen $\mathfrak{a}\mathfrak{A} + \mathfrak{a}'\mathfrak{A}' + \mathfrak{a}''\mathfrak{A}'' = 1$ y para abreviar escribamos k para $\mathfrak{a}\mathfrak{B} + \mathfrak{a}'\mathfrak{B}' + \mathfrak{a}''\mathfrak{B}''$. Entonces a partir de las últimas tres ecuaciones (R) se sigue que $\mathfrak{a}\beta + \mathfrak{a}'\beta' + \mathfrak{a}''\beta'' = \lambda + \mu k$ y de esto es inmediatamente evidente que se da sólo un valor de λ entre los límites de 0 y $\mu - 1$. Cuando hemos hecho esto, los valores de $\mathfrak{B}$, $\mathfrak{B}'$ y $\mathfrak{B}''$ también se habrán determinado, así que resta sólo mostrar que siempre serán enteros. Ahora tenemos

$$\begin{aligned} \mathfrak{B} = \frac{1}{\mu}(\beta - \lambda\mathfrak{A}) &= \frac{1}{\mu}\Big(\beta(1 - \mathfrak{a}\mathfrak{A}) - \mathfrak{A}(\mathfrak{a}'\beta' + \mathfrak{a}''\beta'')\Big) + \mathfrak{A}k \\ &= \frac{1}{\mu}\Big(\mathfrak{a}''(\mathfrak{A}''\beta - \mathfrak{A}\beta'') - \mathfrak{a}'(\mathfrak{A}\beta' - \mathfrak{A}'\beta)\Big) + \mathfrak{A}k \\ &= \frac{1}{e}\Big(\mathfrak{a}''(\alpha''\beta - \alpha\beta'') - \mathfrak{a}'(\alpha\beta' - \alpha'\beta)\Big) + \mathfrak{A}k \end{aligned}$$

Es claro que $\mathfrak{B}$ es un entero, y de la misma manera podemos mostrar que $\mathfrak{B}'$ y $\mathfrak{B}''$ son enteros. De estos argumentos vemos que no puede haber ninguna representación impropia de la forma φ por f que pertenezca al divisor e^2 que no se pueda obtener unívocamente por el método que hemos utilizado.

Si tratamos los restantes divisores cuadrados de D de la misma manera y desarrollamos las representaciones pertenecientes a cada uno de ellos, tendremos todas las representaciones impropias de la forma φ por f.

A partir de esta solución es fácil deducir que el teorema enunciado al final del artículo anterior para las representaciones propias también se aplica a las representaciones impropias; eso es, en general ninguna forma binaria positiva con determinante negativo puede ser representada por una forma ternaria negativa, etc. Pues, si φ fuera una forma binaria tal que de acuerdo con el teorema no pudiera ser representada propiamente por f, entonces todas las formas con determinante $\frac{D}{e^2}$, $\frac{D}{e'^2}$ etc. que φ implica, tampoco podrían ser representadas propiamente por f. La razón es que todas estas formas tienen determinante del mismo signo que φ, y cuando estos determinantes son negativos, todas las formas serán positivas o negativas según φ pertenezca a formas positivas o negativas.

285.

Podemos dar aquí sólo algunos detalles respecto al tercer problema (al cual hemos reducido los dos primeros); o sea respecto a la manera de juzgar si dos formas ternarias dadas del mismo determinante son o no equivalentes y, si lo son, de que manera encontrar todas las transformaciones de una en la otra. La razón es que la solución completa, tal como las obtenidas para problemas análogos de formas binarias, presentaría mayores dificultades aquí. Por lo tanto limitaremos nuestra discusión a algunos casos particulares pertinentes a esta divagación.

I. Para el determinante $+1$ mostramos anteriormente que todas las formas ternarias están repartidas en dos clases, una que contiene todas las formas indefinidas, la otra que contiene todas las formas definidas (negativas). Inmediatamente se concluye que dos formas ternarias cualesquiera de determinante 1 son equivalentes si ambas son definidas o ambas indefinidas; si una es definida y la otra indefinida, no son equivalentes (es claro que la última parte de la proposición es válida para el caso general de formas de cualquier determinante). Similarmente, dos formas cualesquiera con determinante -1 son ciertamente equivalentes si ambas son definidas o ambas indefinidas. Dos formas definidas con determinante 2 son siempre equivalentes; dos

formas indefinidas no son equivalentes si en una los tres primeros coeficientes son todos pares y en la otra no son todos pares; en los casos restantes (los tres primeros coeficientes de ambas formas son todos pares o alguno de los tres primeros coeficientes de ambas formas es impar) las formas serán equivalentes. Podríamos mostrar muchas más proposiciones de este carácter especial si se hubieran desarrollado más ejemplos anteriormente (art. 277).

II. Para todos estos casos se puede encontrar una transformación de una de las formas ternarias equivalentes f y f' en la otra. Pues en todos los casos, en cualquier clase de forma ternaria hemos encontrado un número suficientemente pequeño de formas tales que cualquier forma de la misma clase pueda ser reducida por métodos uniformes a una de ellas; y también hemos mostrado cómo reducirlas todas a una sola forma. Sea F esta forma de la misma clase que f y f'; por los métodos dados anteriormente se puede encontrar transformaciones de las formas f y f' en F y de la forma F en f y f'. Entonces por el artículo 270 pueden deducirse las transformaciones de la forma f en f' y de la forma f' en f.

III. Entonces solamente queda demostrar cómo obtener todas las posibles transformaciones a partir de una transformación de una forma ternaria f en otra f'. Este problema depende de un problema más sencillo, el de encontrar todas las transformaciones de la forma ternaria f en sí misma. Pues si f se transforma en sí misma por varias sustituciones (τ), (τ'), (τ''), etc. y si se transforma en f' mediante la sustitución (t), es claro que se combina la transformación (t) con (τ), (τ'), (τ''), etc. de acuerdo con la norma del artículo 270 para producir transformaciones, cada una de las cuales llevará f hacia f'. Mediante cálculos adicionales, es fácil probar que cualquier transformación de la forma f en f' puede deducirse de esta manera, combinando una transformación dada (t) de f en f' junto con una (y *sólo* una) transformación de la forma f en sí misma. Así a partir de la combinación de una transformación dada de f en f' con *todas* las transformaciones de f en sí misma, se obtienen *todas* las transformaciones de la forma f en f', cada una de ellas sólo una vez.

Restringiremos nuestra investigación de todas las transformaciones de la forma f en sí misma al caso donde f es una forma definida cuyo 4^o, 5^o y 6^o coeficientes son todos $= 0$*). Por lo tanto sea $f = \begin{pmatrix} a, & a', & a'' \\ 0, & 0, & 0 \end{pmatrix}$, y represéntense las sustituciones

*) Los otros casos en los que f es una forma definida se pueden reducir a éste; pero si f es una forma indefinida, debe usarse un método completamente diferente y el número de transformaciones será infinito.

mediante las cuales f es transformada en sí misma por

$$\begin{array}{lll} \alpha, & \beta, & \gamma \\ \alpha', & \beta', & \gamma' \\ \alpha'', & \beta'', & \gamma'' \end{array}$$

así que las siguientes ecuaciones se cumplen

$$\begin{aligned} a\alpha^2 + a'\alpha'^2 + a''\alpha''^2 &= a \\ a\beta^2 + a'\beta'^2 + a''\beta''^2 &= a' \\ a\gamma^2 + a'\gamma'^2 + a''\gamma''^2 &= a'' \\ a\alpha\beta + a'\alpha'\beta' + a''\alpha''\beta'' &= 0 \\ a\alpha\gamma + a'\alpha'\gamma' + a''\alpha''\gamma'' &= 0 \\ a\beta\gamma + a'\beta'\gamma' + a''\beta''\gamma'' &= 0 \end{aligned} \qquad (\Omega)$$

Ahora deben distinguirse tres casos:

I. Cuando a, a' y a'' (que tienen el mismo signo) son todos diferentes, supongamos que $a < a'$ y $a' < a''$ (si hay un orden diferente de magnitud, las mismas conclusiones resultarán de manera similar). Entonces la primera ecuación en (Ω) evidentemente requiere que $\alpha' = \alpha'' = 0$, por lo tanto $\alpha = \pm 1$; entonces por las ecuaciones 4 y 5 resulta $\beta = 0$, $\gamma = 0$; similarmente de la ecuación 2 tenemos $\beta'' = 0$ y por lo tanto $\beta' = \pm 1$; ahora a partir de la ecuación 6, $\gamma' = 0$ y de la 3, $\gamma'' = \pm 1$ así pues (debido a la ambigüedad independiente de los signos) habrá en total 8 transformaciones.

II. Cuando dos de los números a, a' y a'' son iguales e.g., $a' = a''$ y el tercero diferente, supongamos:

Primero que $a < a'$. Entonces de la misma manera que en el caso anterior tendremos que $\alpha' = 0$, $\alpha'' = 0$, $\alpha = \pm 1$, $\beta = 0$, $\gamma = 0$; y a partir de las ecuaciones 2, 3 y 6 es fácil deducir que o $\beta' = \pm 1$, $\gamma' = 0$, $\beta'' = 0$, $\gamma'' = \pm 1$ ó $\beta' = 0$, $\gamma' = \pm 1$, $\beta'' = \pm 1$, $\gamma'' = 0$.

Pero si, *en segundo lugar*, $a > a'$, se obtienen las mismas conclusiones de esta manera; a partir de las ecuaciones 2 y 3 resulta necesariamente $\beta = 0$, $\gamma = 0$ y además tenemos $\beta' = \pm 1$, $\gamma' = 0$, $\beta'' = 0$, $\gamma'' = \pm 1$ o $\beta' = 0$, $\gamma' = \pm 1$, $\beta'' = \pm 1$, $\gamma'' = 0$; en cualquier caso, a partir de las ecuaciones 4 y 5 tendremos $\alpha' = 0$, $\alpha'' = 0$ y a partir de la 1, $\alpha = \pm 1$. Y así para cada caso habrá 16 transformaciones diferentes. Los

dos restantes casos donde $a = a''$ o $a = a'$ se pueden resolver de manera totalmente similar. En el primer caso necesitamos simplemente intercambiar los caracteres α, α', α'' con β, β', β'' respectivamente; en el segundo caso se tienen que intercambiar con γ, γ', γ'' respectivamente.

III. Cuando todos los a, a' y a'' son iguales, las ecuaciones 1, 2 y 3 requieren que en cada uno de los tres triples α, α', α''; β, β', β''; γ, γ', γ'' dos de los números sean $= 0$, y el tercero $= \pm 1$. Mediante las ecuaciones 4, 5 y 6 es fácil ver que sólo uno de los tres números α, β y γ puede ser $= \pm 1$. Lo mismo es cierto de los conjuntos α', β', γ' y α'', β'', γ''. Por lo tanto sólo hay seis posibles combinaciones:

$$\begin{array}{|ccccccc|l} \alpha & \alpha & \alpha' & \alpha' & \alpha'' & \alpha'' & = \pm 1 \\ \beta' & \beta'' & \beta & \beta'' & \beta & \beta' & = \pm 1 \\ \gamma'' & \gamma' & \gamma'' & \gamma & \gamma' & \gamma & = \pm 1 \end{array} \qquad \text{Los restantes seis coeficientes serán } = 0$$

y, por causa de la ambigüedad de signos, hay un total de 48 transformaciones. La misma tabla también incluye los casos anteriores, pero solamente se debe tomar la primera columna cuando a, a' y a'' son todos diferentes; la primera y segunda cuando $a' = a''$; la primera y tercera cuando $a = a'$; la primera y sexta cuando $a = a''$.

En resumen, si la forma $f = ax^2 + a'x'^2 + a''x''^2$ se transforma en una forma equivalente f' mediante la sustitución

$$x = \delta y + \varepsilon y' + \zeta y'', \quad x' = \delta' y + \varepsilon' y' + \zeta' y'', \quad x'' = \delta'' y + \varepsilon'' y' + \zeta'' y''$$

toda transformación de la forma f en f' estará comprendida en el siguiente esquema:

$$\begin{array}{|ccccccc|l} x & x' & x' & x' & x'' & x'' & = \pm(\delta y & + \varepsilon y' & + \zeta y'') \\ x' & x'' & x & x'' & x & x' & = \pm(\delta' y & + \varepsilon' y' & + \zeta' y'') \\ x'' & x' & x'' & x & x' & x & = \pm(\delta'' y & + \varepsilon'' y' & + \zeta'' y'') \end{array}$$

con esta diferencia: que las seis columnas serán utilizadas en su totalidad cuando $a = a' = a''$; las columnas 1 y 2 cuando $a' = a''$ con a distinto; 1 y 3 cuando $a = a'$; 1 y 6 cuando $a = a''$; y la primera sola cuando a, a' y a'' son todos diferentes. En el primer caso, el número de transformaciones será 48, en el segundo, tercero y cuarto 16, y en el quinto 8.

ALGUNAS APLICACIONES A LA TEORIA DE LAS FORMAS BINARIAS.

Encontrar una forma cuya duplicación produce una forma dada del género principal.

Puesto que los elementos básicos de la teoría de formas ternarias se han desarrollado de manera concisa, procederemos a algunas aplicaciones especiales. Entre ellas, el siguiente problema merece el primer lugar.

286.

PROBLEMA. *Dada una forma binaria $F = (A,\ B,\ C)$ de determinante D que pertenece al género principal: encontrar una forma binaria f cuya duplicación nos da F.*

Solución. I. Sea F' la opuesta de la forma F. Se busca una representación propia de $F' = AT^2 - 2BTU + CU^2$ por la forma ternaria $x^2 - 2yz$. Suponga que es

$$x = \alpha T + \beta U, \qquad y = \alpha' T + \beta' U, \qquad z = \alpha'' T + \beta'' U.$$

Es claro que esto se puede realizar a partir de la teoría anterior sobre formas ternarias, ya que, por hipótesis, F pertenece al género principal, así que hay un valor para la expresión $\sqrt{(A,B,C)}$ (mod. D), a partir del cual se puede encontrar una forma ternaria φ de determinante 1 en la cual $(A,-B,C)$ será una parte y todos sus coeficientes serán enteros. Es igualmente obvio que φ será una forma indefinida (pues por hipótesis F ciertamente no es una forma negativa); y por lo tanto será necesariamente equivalente a la forma $x^2 - 2yz$. Por consiguiente, se podrá encontrar una transformación de ésa a φ, la cual da una representación propia de la forma F' por la forma $x^2 - 2yz$. Como resultado

$$A = \alpha^2 - 2\alpha'\alpha'', \qquad -B = \alpha\beta - \alpha'\beta'' - \alpha''\beta', \qquad C = \beta^2 - 2\beta'\beta''$$

además, designando los números $\alpha\beta' - \alpha'\beta$, $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$ por a, b, c respectivamente, éstos no tendrán un divisor común y $D = b^2 - 2ac$.

II. Con la ayuda de la última observación del artículo 235, es fácil concluír que F, mediante la sustitución $2\beta'$, β, β, β''; $2\alpha'$, α, α, α'', se transformará en el producto de la forma $(2a,-b,c)$ con ella misma, y por la sustitución β', β, β, $2\beta''$; α', α, α, $2\alpha''$, en el producto de la forma $(a,-b,2c)$ con ella misma. Ahora el máximo común divisor de los números $2a$, $2b$ y $2c$ es 2; por lo tanto si el número c es

impar, los números $2a$, $2b$ y c no tendrán un divisor común, así $(2a, -b, c)$ será una forma propiamente primitiva; similarmente si a es impar $(a, -b, 2c)$ será una forma propiamente primitiva. En el primer caso F será obtenida a partir de la duplicación de la forma $(2a, -b, c)$ y en segundo caso a partir de una duplicación de la forma $(a, -b, 2c)$ (ver conclusión 4, art. 235). Ciertamente uno de estos casos siempre se cumplirá. En efecto, si ambas a y c fueran pares, b sería necesariamente impar; ahora es fácil confirmar que $\beta''a + \beta b + \beta' c = 0$, $\alpha''a + \alpha b + \alpha' c = 0$ y se sigue que βb y αb serán pares y así también lo serán α y β. De esto seguiría que A y C son pares pero esto contradice a la hipótesis según la cual F es una forma del género principal y así de orden propiamente primitiva. Pero puede ocurrir que a y c sean impares. En este caso inmediatamente habrá dos formas que producirán F mediante su duplicación.

Ejemplo. Propóngase la forma $F = (5, 2, 31)$ con determinante -151. Un valor de la expresión $\sqrt{(5, 2, 31)}$ será $(55, 22)$; por los métodos del artículo 272 encontramos que la forma ternaria $\varphi = \left(\begin{smallmatrix} 5, & 31, & 4 \\ 11, & 0, & -2 \end{smallmatrix}\right)$ es equivalente a la forma $\left(\begin{smallmatrix} 1, & 1, & -1 \\ 0, & 0, & 0 \end{smallmatrix}\right)$ y ésta se transformará en φ mediante la sustitución $\left\{\begin{matrix} 2, & 2, & 1 \\ 1, & -6, & -2 \\ 0, & 3, & 1 \end{matrix}\right\}$; y con la ayuda de las transformaciones dadas en el artículo 277 encontramos que $\left(\begin{smallmatrix} 1, & 0, & 0 \\ -1, & 0, & 0 \end{smallmatrix}\right)$ es transformada en φ por la sustitución $\left\{\begin{matrix} 3, & -7, & -2 \\ 2, & -1, & 0 \\ 1, & -9, & -3 \end{matrix}\right\}$. Así pues $a = 11$, $b = -17$, $c = 20$; por lo tanto puesto que a es impar, F se obtendrá de la duplicación de la forma $(11, 17, 40)$ y se transformará en el producto de esta forma con ella misma por la sustitución -1, -7, -7, -18; 2, 3, 3, 2.

287.

Agregamos las siguientes observaciones sobre el problema que se resolvió en el artículo anterior.

I. Si la forma F es transformada en un producto de las dos formas (h, i, k) y (h', i', k') por la sustitución p, p', p'', p'''; q, q', q'', q''' (supongamos que cada una se toma propiamente) se tendrán las siguientes ecuaciones que son fácilmente deducidas

de la conclusión 3 del artículo 235:

$$\begin{aligned} p''hn' - p'h'n - p(in' - i'n) &= 0 \\ (p'' - p')(in' + i'n) - p(kn' - k'n) + p'''(hn' - h'n) &= 0 \\ p'kn' - p''k'n - p'''(in' - i'n) &= 0 \end{aligned}$$

y tres más que se derivan de éstas intercambiando los números p, p', p'', p''' y q, q', q'', q'''; n y n' son las raíces cuadradas positivas que resultan de la división de los determinantes de las formas (h, i, k) y (h', i', k') por el determinante de la forma F. Así, si estas formas son idénticas, eso es, $n = n'$, $h = h'$, $i = i'$, $k = k'$, las ecuaciones serán

$$(p'' - p')hn = 0, \qquad (p'' - p')in = 0, \qquad (p'' - p')kn = 0$$

y *necesariamente* $p' = p''$ y similarmente $q' = q''$. Por lo tanto, asignando a las formas (h, i, k) y (h', i', k') las *mismas* incógnitas t y u y designando las incógnitas de F por T y U, entonces F será transformada por la sustitución

$$T = pt^2 + 2p'tu + p'''u^2, \qquad U = qt^2 + 2q'tu + q'''u^2 \quad \text{en} \quad (ht^2 + 2itu + ku^2)^2$$

II. Si la forma F se obtiene a partir de una duplicación de la forma f, será también obtenida a partir de una duplicación de cualquier otra forma contenida en la misma clase que f; eso es, la clase de la forma F se obtendrá a partir de una duplicación de la clase de la forma f (ver art. 238). Así en el ejemplo del artículo anterior, $(5, 2, 31)$ también se obtendrá de una duplicación de la forma $(11, -5, 16)$ la cual es propiamente equivalente a la forma $(11, 17, 40)$. A partir de una clase que por duplicación produce a la clase de la forma F, se encuentran *todas* (si hay más que una) aquellas clases con la ayuda del problema 260; en nuestro ejemplo no hay ninguna otra clase positiva porque existe sólo una clase ambigua positiva propiamente primitiva de determinante -151 (la clase principal); y puesto que, a partir de la composición de la única clase ambigua negativa $(-1, 0, -151)$ con la clase $(11, -5, 16)$ resulta la clase $(-11, -5, -16)$, ésta será la única clase negativa y de su duplicación resulta la clase $(5, 2, 31)$.

III. Puesto que por la solución del problema del artículo anterior queda claro que cualquier clase propiamente primitiva (positiva) de formas binarias perteneciendo al género principal se puede obtener de la duplicación de alguna clase propiamente primitiva del mismo determinante, podemos ampliar el teorema del artículo 261. Este teorema afirmaba que podríamos estar seguros de que *al menos* la mitad de todos los

caracteres asignables para un determinante no cuadrado D no pueden corresponder a géneros propiamente primitivos (positivos). Ahora podemos decir que *exactamente* la mitad de todos estos caracteres corresponden a tales géneros y ninguno de los de la otra mitad puede corresponder a ellos (ver demostración del teorema). En el artículo 264 distribuimos todos esos caracteres entre dos grupos iguales P y Q. Se probó que ninguno de los de Q puede corresponder a formas propiamente primitivas (positivas). Aún se dudaba de si había géneros que correspondían a cada uno de los caracteres de P. Ahora la duda se ha aclarado y estamos seguros de que entre el conjunto completo de caracteres de P no hay ninguno que no corresponda a un género. Se mostró en el artículo 264, I que para un determinante negativo es imposible para P y *sólo* posible para Q el tener miembros en un orden *negativo* propiamente primitivo. Mostraremos en efecto que *todos* los miembros de Q son posibles. Si K es cualquier carácter en Q, f una forma arbitraria en el orden de formas negativas propiamente primitivas de determinante D, y K' su carácter, entonces K' estará en Q; a partir de esto es fácil ver que el carácter compuesto por K y K' (según la norma del art. 246) pertenece a P y entonces hay formas propiamente primitivas positivas de determinante D que le corresponden. La composición de esta forma con f da raíz a una forma propiamente primitiva negativa de determinante D cuyo carácter será K. De manera similar se prueba que aquellos caracteres en un orden impropiamente primitivo, que según los métodos de los artículos 264 II, III resultan ser los *únicos* posibles, son realmente del *todo* posibles, independientemente de si pertenecen a P o a Q. Creemos que estos teoremas están entre los más bellos de la teoría de las formas binarias, especialmente porque, a pesar de ser sumamente simples, son tan profundos que sus demostraciones rigurosas requieren de muchas otras investigaciones.

La teoría de la descomposición de números y formas binarias en tres cuadrados.

Veamos ahora otra aplicación de la divagación anterior, la descomposición de números y formas binarias en tres cuadrados. Empezamos con lo siguiente.

288.

PROBLEMA. *Dado un número positivo M, encontrar los requisitos que formas binarias primitivas negativas de determinante $-M$ deben satisfacer para que sean residuos cuadráticos de M, eso es, para que tengan* 1 *como un número característico.*

Solución. Designemos por Ω el conjunto de todos los caracteres particulares que dan las relaciones del número 1 tanto a los divisores primos (impares) de M como a los números 8 ó 4 cuando divide a M. Estos caracteres serán Rp, Rp', Rp'', etc., donde p, p', p'', etc. son los divisores primos, y 1, 4 cuando 4 divide a M; 1, 8 cuando 8 divide a M. Además utilizaremos las letras P y Q con el mismo significado que en el artículo anterior y en el artículo 264. Ahora distinguimos los siguientes casos.

I. Cuando M es divisible por 4, Ω será un carácter completo, y es claro por el artículo 233 V que 1 puede ser un número característico solamente de aquellas formas cuyo carácter es Ω. Pero es claro que Ω es el carácter de la forma principal $(1, 0, M)$ y así pertenece a P y no puede resultar de una forma propiamente primitiva negativa; por lo tanto, puesto que no hay formas impropiamente primitivas para este determinante, en este caso no habrá formas primitivas negativas que sean residuos de M.

II. Cuando $M \equiv 3 \pmod 4$ el mismo razonamiento es válido con la excepción de que en este caso existe un orden *impropiamente* primitivo negativo en el cual los caracteres P serán posibles o no según $M \equiv 3$ ó $M \equiv 7 \pmod 8$ (ver art. 264 III). En el primer caso habrá un género para este orden cuyo carácter es Ω, así 1 será el número característico de todas las formas contenida en ella; en el segundo caso no puede haber ninguna forma negativa con esta propiedad.

III. Cuando $M \equiv 1 \pmod 4$, Ω aún no es un carácter completo, pero debemos agregarle una relación con el número 4; es claro sin embargo, que Ω debe pertenecer al carácter de una forma cuyo número característico es 1, y recíprocamente cualquier forma cuyo carácter es ó Ω; 1, 4, ó Ω; 3, 4, tiene 1 como número característico. Ahora Ω; 1, 4 es claramente el carácter del género principal que pertenece a P y por lo tanto es imposible dentro de un orden propiamente primitivo negativo; por la misma razón Ω; 3, 4 pertenecerá a Q (art. 263). Por esto habrá un género correspondiente al orden propiamente primitivo negativo de todas aquellas formas que tendrán 1 como número característico. En este caso, tal como en el siguiente no habrá ningún orden impropiamente primitivo.

IV. Cuando $M \equiv 2 \pmod 4$ debemos agregarle a Ω una relación con 8 para obtener un carácter completo. Estas relaciones serán 1 *y* 3, 8 ó 5 *y* 7, 8 cuando $M \equiv 2 \pmod 8$; y ó 1 *y* 7, 8 ó 3 *y* 5, 8 cuando $M \equiv 6 \pmod 8$. En el primer caso el carácter Ω; 1 *y* 3, 8 evidentemente pertenecerán a P y así Ω; 5 *y* 7, 8 a Q. Como consecuencia de esto, habrá un género propiamente primitivo negativo que le corresponde. Por una razón similar, en el segundo caso habrá un género en el orden

propiamente primitivo negativo, cuya forma tiene la propiedad prescrita; eso es, su carácter es Ω; 3 y 5, 8.

A partir de todo eso se sigue que no hay formas primitivas negativas de determinante $-M$ con número característico 1 excepto cuando M es congruente con uno de los números 1, 2, 3, 5 ó 6 según el módulo 8 y ellos pertenecerán a sólo un género, que es impropio cuando $M \equiv 3$; no hay tales formas cuando $M \equiv 0$, 4 ó 7 (mod. 8). Pero si $(-a, -b, -c)$ es una forma primitiva negativa con número característico $+1$, (a, b, c) será una forma primitiva positiva con número característico -1. De esto es claro que en los cinco casos anteriores (cuando $M \equiv 1$, 2, 3, 5, 6) hay un género primitivo positivo cuyas formas tienen número característico -1, y es *impropio* si $M \equiv 3$; sin embargo en el último de los tres casos (cuando $M \equiv 0$, 4, 7) no hay tales formas positivas.

289.

En cuanto a las representaciones propias de las formas binarias por la forma ternaria $x^2 + y^2 + z^2 = f$, podemos obtener lo siguiente a partir de la teoría general del artículo 282.

I. La forma binaria φ no se puede representar propiamente por f a menos que sea una forma positiva primitiva y -1 (i.e., el determinante de la forma f) sea su número característico. Así para un determinante positivo y además para un determinante negativo $-M$, cuando M es divisible por 4 o es de la forma $8n + 7$, no hay formas binarias propiamente representables por f.

II. Ahora si $\varphi = (p, q, r)$ es una forma positiva primitiva de determinante $-M$, y -1 es un número característico de la forma φ y también de la forma opuesta $(p, -q, r)$, habrá una representación propia de la forma φ por f que pertenece a cualquier valor de la expresión $\sqrt{-(p, -q, r)}$. Eso es, todos los coeficientes de la forma ternaria g de determinante -1 (art. 283) necesariamente serán enteros, la forma g será definida y así equivalente a f (art. 285.I).

III. Por el artículo 283.III el número de representaciones que pertenecen al mismo valor de la expresión $\sqrt{-(p, -q, r)}$ en todos los casos, excepto cuando $M = 1$ y $M = 2$, es igual en magnitud al número de transformaciones de la forma f en g, y así, por el artículo 285, $= 48$; así si se conoce una representación que pertenece a un valor dado, los 47 restantes se pueden obtener a partir de ella permutando los valores de x, y, z en todas las maneras posibles y cambiando sus signos; como resultado,

las 48 representaciones presentarán *una sola* descomposición de la forma φ en tres cuadrados, si consideramos los cuadrados en sí y no su orden o el signo de sus raíces.

IV. Sea μ el número de todos los enteros primos impares diferentes que dividen a M; no es difícil concluir del artículo 233 que el número de valores diferentes de la expresión $\sqrt{-(p,-q,r)}$ (mod. M) será $= 2^\mu$, donde, según el artículo 283, necesitamos considerar sólo la mitad de éstos (cuando $M > 2$). Por lo tanto el número de todas las representaciones propias de la forma φ por f será $= 48 \cdot 2^{\mu-1} = 3 \cdot 2^{\mu+3}$; pero el número de descomposiciones diferentes en tres cuadrados es $= 2^{\mu-1}$.

Ejemplo. Sea $\varphi = 19t^2 + 6tu + 41u^2$, de modo que $M = 770$; aquí se debe considerar (art. 283) los cuatro valores siguientes de la expresión $\sqrt{-(19,-3,41)}$ (mod. 770): $(39, 237)$, $(171, -27)$, $(269, -83)$, $(291, -127)$. Para encontrar las representaciones que pertenecen a los valores $(39, 237)$, debemos determinar la forma ternaria $\left(\begin{smallmatrix} 19, & 41, & 2 \\ 3, & 6, & 3 \end{smallmatrix}\right) = g$. Mediante los métodos de los artículos 272 y 275, encontramos que f se transformará en esta forma por la sustitución

$$\left\{\begin{array}{rrr} 1, & -6, & -0 \\ -3, & -2, & -1 \\ -3, & -1, & -1 \end{array}\right\}$$

y la representación de la forma φ por f es:

$$x = t - 6u, \qquad y = -3t - 2u, \qquad z = -3t - u$$

Por razones de brevedad no escribiremos las 47 representaciones restantes que pertenecen a ese mismo valor, las cuales resultan de las permutaciones de estos valores y el cambio de signos. Todas las 48 representaciones producen la misma descomposición de la forma φ en tres cuadrados

$$t^2 - 12tu + 36u^2, \qquad 9t^2 + 12tu + 4u^2, \qquad 9t^2 + 6tu + u^2.$$

De manera similar el valor $(171, -27)$ dará una descomposición en cuadrados $(3t + 5u)^2$, $(3t - 4u)^2$, t^2; el valor $(269, -83)$ dará $(t + 6u)^2 + (3t + u)^2 + (3t - 2u)^2$; y finalmente el valor $(291, -127)$ dará $(t + 3u)^2 + (3t + 4u)^2 + (3t - 4u)^2$; cada una de estas descomposiciones es equivalente a 48 representaciones. Fuera de estas 192 representaciones o cuatro descomposiciones no hay otras, puesto que 770 no es divisible por ningún cuadrado y por lo tanto no puede haber ninguna representación impropia.

290.

Las formas de determinante -1 y -2 están sujetas a ciertas excepciones, así que diremos un poco sobre ellas como caso particular. Empezamos con la observación general de que si φ y φ' son dos formas binarias equivalentes cualesquiera, (Θ) una transformación dada de la primera en la segunda, entonces combinando cualquiera de las representaciones de φ por la forma ternaria f con la sustitución (Θ), se obtiene una representación de la forma φ' por f. Además a partir de las representaciones propias de φ obtenemos las representaciones propias de la forma φ', a partir de representaciones distintas de φ obtenemos representaciones distintas de φ' y si tomamos todas las representaciones de la primera obtendremos todas las representaciones de la segunda. Todo esto se puede comprobar mediante cálculos muy sencillos. Por lo tanto una de las formas φ y φ' es representable por f de tantas maneras distintas como lo es la otra.

I. Primero sea $\varphi = t^2 + u^2$ y φ' una forma binaria positiva cualquiera de determinante -1, a la cual φ es equivalente. Sea $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$ la sustitución que transforma φ en φ'. La forma φ se representa por la forma ternaria $f = x^2 + y^2 + z^2$, poniendo $x = t$, $y = u$, $z = 0$; permutando x, y, z resultan *seis* representaciones, y a partir de cada una de éstas, cuatro más cambiando los signos de t y u. Así pues habrá en total 24 representaciones que corresponden a sólo una descomposición en tres cuadrados. Es fácil ver que no habrá ninguna otra representación salvo éstas. Y se concluye que la forma φ' se puede descomponer en tres cuadrados de sólo una manera, a saber, $(\alpha t' + \beta u')^2$, $(\gamma t' + \delta u')^2$ y 0. Esta descomposición será equivalente a las 24 representaciones.

II. Sea $\varphi = t^2 + 2u^2$, φ' cualquier otra forma binaria positiva de determinante -2, en la cual se transforma φ mediante la sustitución $t = \alpha t' + \beta u'$, $u = \gamma t' + \delta u'$. Entonces de manera similar que en el caso anterior concluimos que φ y también φ' se pueden descomponer en tres cuadrados de manera única, a saber, φ en $t^2 + u^2 + u^2$ y φ' en $(\alpha t' + \beta u')^2 + (\gamma t' + \delta u')^2 + (\gamma t' + \delta u')^2$; es obvio que esta descomposición es equivalente a las 24 representaciones.

De todo esto se sigue que las formas binarias de determinante -1 y -2 en cuanto al número de representaciones por la forma ternaria $x^2 + y^2 + z^2$ son completamente iguales a las otras formas binarias; puesto que en ambos casos tenemos $\mu = 0$, la fórmula dada en IV del artículo anterior dará las 24 representaciones. La razón para esto es que las dos excepciones a las cuales están sujetas estas formas se compensan mutuamente.

Por razones de brevedad omitiremos la aplicación, a la forma $x^2 + y^2 + z^2$, de la teoría general respecto a representaciones impropias dada en el artículo 284.

291.

El problema de encontrar todas las representaciones propias de un *número* positivo M por la forma $x^2 + y^2 + z^2$ se reduce primeramente en el artículo 281 a la investigación de las representaciones propias del número $-M$ por la forma $-x^2 - y^2 - z^2 = f$; por los métodos del artículo 280 éstas se pueden encontrar de la siguiente manera.

I. Encontramos todas las clases de formas binarias de determinante $-M$ cuyas formas se pueden representar propiamente por $X^2 + Y^2 + Z^2 = F$ (la cual tiene a f como adjunta). Cuando $M \equiv 0$, 4 ó 7 (mod. 8), por el artículo 288 no hay tales clases y entonces M no se puede descomponer en tres cuadrados que no tienen un divisor común *). Pero cuando $M \equiv 1$, 2, 5 ó 6, habrá un género positivo propiamente primitivo, y cuando $M \equiv 3$ uno impropiamente primitivo que incluye todas aquellas clases. Designemos el número de estas clases por k.

II. Ahora escoja arbitrariamente una forma de cada una de estas k clases y llámelas φ, φ', φ'', etc.; investigue todas las representaciones propias de cada una de éstas por F. El número de ellas será $3 \cdot 2^{\mu+3}k = K$, donde μ es el número de factores primos (impares) de M; finalmente a partir de cada una de estas representaciones, tales como

$$X = mt + nu, \qquad Y = m't + n'u, \qquad Z = m''t + n''u$$

derivamos la siguiente representación de M por $x^2 + y^2 + z^2$:

$$x = m'n'' - m''n', \qquad y = m''n - mn'', \qquad z = mn' - m'n$$

Todas las representaciones de M están contenidas en el conjunto, que designaremos por Ω, de estas K representaciones.

III. Sólo queda determinar si hay algunas representaciones en Ω que sean *idénticas*; y puesto que del artículo 280.III está claro que aquellas representaciones

*) Esta imposibilidad es también clara por el hecho de que la suma de tres cuadrados impares debe ser $\equiv 3$ (mod. 8); la suma de dos impares con uno par es $\equiv 2$ ó $\equiv 6$; la suma de un impar y dos pares es $\equiv 1$ ó $\equiv 5$; y finalmente la suma de tres pares es $\equiv 0$ ó $\equiv 4$; pero en el último caso la representación es claramente impropia.

en Ω que se obtienen de diferentes formas, e.g., de φ y φ' deben ser distintas, la única pregunta que queda es si diferentes representaciones de la misma forma e.g., φ por F pueden dar lugar a representaciones idénticas del número M por $x^2+y^2+z^2$. Ahora es inmediatamente evidente que si entre las representaciones de φ encontramos

$$X = mt + nu, \qquad Y = m't + n'u, \qquad Z = m''t + n''u \tag{r}$$

también encontraremos entre las mismas representaciones

$$X = -mt - nu, \qquad Y = -m't - n'u, \qquad Z = -m''t - n''u \tag{r'}$$

y a partir de cada una podemos obtener la misma representación de M que llamaremos (R); examinemos por lo tanto si la representación (R) puede obtenerse todavía de otras representaciones de φ. A partir del artículo 280.III, si hacemos que $\chi = \varphi$ y si exhibimos todas las transformaciones de la forma propia φ en sí misma por

$$t = \alpha t + \beta u, \qquad u = \gamma t + \delta u$$

podemos deducir que todas aquellas representaciones de la forma φ a partir de la cual se obtiene R serán expresadas por

$$\begin{aligned} x &= (\alpha m + \gamma n)t + (\beta m + \delta n)u \\ y &= (\alpha m' + \gamma n')t + (\beta m' + \delta n')u \\ z &= (\alpha m'' + \gamma n'')t + (\beta m'' + \delta n'')u \end{aligned}$$

Pero de la teoría de la transformación de formas binarias con determinante negativo como se explicó en el artículo 179, se sigue que en todos los casos, excepto cuando $M = 1$ y $M = 3$, hay sólo dos transformaciones propias de la forma φ es sí misma, a saber, α, β, γ, $\delta = 1, 0, 0, 1$ y $= -1, 0, 0, -1$ respectivamente (pues como φ es una forma primitiva, el número que designamos en el artículo 179 por m será ó 1 ó 2 y así, excepto en los casos que se excluyeron, 1) ciertamente será aplicable). Por lo tanto (R) puede aparecer sólo a partir de r, r' y cada una de las representaciones propias del número M se encontrará dos veces, y no más en Ω; y el número de representaciones propias de M será $\frac{1}{2}K = 3 \cdot 2^{\mu+2}k$.

En cuanto a los casos que se excluyeron, el número de transformaciones propias de φ en sí misma, con base en el artículo 179 serán 4 para $M = 1$ y 6 para $M = 3$; y es fácil comprobar que el número de representaciones propias de los números 1 y

3 es $\frac{1}{4}K$ y $\frac{1}{6}K$ respectivamente; eso es cada número se puede descomponer en tres cuadrados de una manera única, 1 en $1+0+0$, 3 en $1+1+1$. La descomposición de 1 proporciona seis, la descomposición de 3, ocho representaciones diferentes, ahora para $M=1$ tenemos $K=24$ (aquí $\mu=0$, $k=1$) y para $M=3$ tenemos $K=48$ (aquí $\mu=1$, $k=1$).

Sea h el número de clases en el género principal. Por artículo 252 será igual al número de clases en cualquier otro género propiamente primitivo. Observamos que $k=h$ para $M\equiv 1,\ 2,\ 5$ ó $6 \pmod 8$, pero $k=\frac{1}{3}h$ para $M\equiv 3 \pmod 8$, excepto en el caso de $M=3$ (donde $k=h=1$). Así, el número de representaciones, *en general*, de números de la forma $8n+3$ es $=2^{\mu+2}h$, puesto que para el número 3 las dos excepciones se compensan entre sí.

292.

Hemos distinguido la descomposición de números (y también de formas binarias) en tres cuadrados por representaciones de la forma $x^2+y^2+z^2$, de tal manera que en el primero nos preocupamos únicamente por la magnitud de los cuadrados y en el segundo también consideramos el orden de las raíces y sus signos. Así, consideramos que las representaciones $x=a$, $y=b$, $z=c$ y $x=a'$, $y=b'$, $z=c'$ son distintas a menos que $a=a'$, $b=b'$, $c=c'$ simultáneamente; y tomamos las descomposiciones en $a^2+b^2+c^2$ y en $a'^2+b'^2+c'^2$ como la misma si, sin considerar el orden, los cuadrados en una son iguales a los cuadrados en la otra. De esto es claro:

I. Que la descomposición del número M en $a^2+b^2+c^2$ es equivalente a 48 representaciones si ninguno de los cuadrados es $=0$ y si todos son distintos entre sí; pero sólo a 24 si alguno es $=0$ y los otros son distintos entre sí, *o* ninguno es $=0$ y dos son iguales. Sin embargo, si en la descomposición de un número dado en tres cuadrados dos de los cuadrados $=0$, *ó* uno $=0$ y los restantes iguales entre sí, *o* todos son iguales entre sí, la descomposición será equivalente a 6 *o* 12 *o* 18 representaciones; pero esto no puede suceder a menos que tengamos el caso especial de $M=1$ o 2 o 3, respectivamente, por lo menos si se quiere que las representaciones sean propias. Excluyendo estos tres casos, supongamos que el número de descomposiciones de un número M en tres cuadrados (que no tienen un divisor común) es E, y que entre ellas tenemos e descomposiciones en las cuales un cuadrado es 0, y e' en las cuales dos cuadrados son iguales; el primero se puede considerar como descomposiciones en dos cuadrados y el segundo como descomposiciones en un cuadrado y dos veces un cuadrado. Entonces el número de representaciones propias del número M por

$x^2 + y^2 + z^2$ será

$$= 24(e + e') + 48(E - e - e') = 48E - 24(e + e')$$

Pero de la teoría de formas binarias es fácil ver que e será $= 0$ ó $= 2^{\mu-1}$, según -1 sea un no residuo o sea un residuo cuadrático de M, y que e' será $2^{\mu-1}$ ó $= 0$ según -2 sea o no un residuo de M. Aquí μ es el número de factores primos (impar) de M (ver art. 182; omitimos aquí una exposición más completa). De todo esto tenemos

$$E = 2^{\mu-2}k, \quad \text{si ambos } -1 \text{ y } -2 \text{ son no residuos de } M;$$
$$E = 2^{\mu-2}(k+2), \quad \text{si ambos números son residuos;}$$
$$E = 2^{\mu-2}(k+1), \quad \text{si uno es un residuo y el otro un no residuo.}$$

En los casos excluidos donde $M = 1$ y $M = 2$ esta fórmula haría que $E = \frac{3}{4}$, mientras que debió haber sido $E = 1$. Sin embargo, para $M = 3$ obtenemos el valor correcto, $E = 1$, porque las excepciones se compensan mutuamente.

Por lo tanto si M es un número primo, resulta $\mu = 1$ y así $E = \frac{1}{2}(k+2)$ cuando $M \equiv 1 \pmod 8$; $E = \frac{1}{2}(k+1)$ cuando $M \equiv 3$ ó $M \equiv 5$. Estos teoremas especiales fueron descubiertos por el ilustre Legendre por métodos de inducción y fueron publicados por él en aquel comentario espléndido que hemos citado a menudo, *Hist. de l'Ac. de Paris* 1785, *p.* 530 y siguientes. Si lo presentó de manera un poco distinta es porque no distinguió entre equivalencias propias e impropias y así mezcló clases opuestas.

II. Para encontrar todas las descomposiciones de un número M en tres cuadrados (sin un divisor común) no es necesario obtener todas las representaciones propias de todas las formas φ, φ' y φ''. En efecto, es fácil comprobar que todas las (48) representaciones de la forma φ que corresponden al mismo valor de la expresión $\sqrt{-(p,-q,r)}$ (donde $\varphi = (p,q,r)$) darán la misma descomposición del número M, así es suficiente si tenemos una de ellas, o lo que es lo mismo, si conocemos todas las descomposiciones *) diferentes de la forma φ en tres cuadrados. Lo mismo es cierto para las restantes φ', φ'', etc. Ahora si φ pertenece a una clase no ambigua, es permitido ignorar la forma que fue escogida de la clase opuesta; eso es, es suficiente considerar sólo una de las dos clases opuestas. Pues, ya que es completamente arbitrario cuál forma seleccionamos de una clase, supongamos que se escoge la forma

*) Siempre debemos entender la palabra "propia" si queremos transferir esta expresión de representaciones a descomposiciones.

φ' de la clase opuesta a la que contiene φ, la cual es opuesta a la forma φ. Entonces no es difícil mostrar que si se representan las descomposiciones propias de la forma φ por la expresión general

$$(gt + hu)^2 + (g't + h'u)^2 + (g''t + h''u)^2$$

todas las descomposiciones de la forma φ' serán expresadas por

$$(gt - hu)^2 + (g't - h'u)^2 + (g''t - h''u)^2$$

y la misma descomposición del número M se obtendrá de ambas. Finalmente, para el caso en el cual φ es de una clase ambigua, pero no de la clase principal ni equivalente a la forma $(2, 0, \frac{1}{2}M)$ o $(2, 1, \frac{1}{2}(M+1))$ (según M sea par o impar), es permitido omitir la mitad de los valores de la expresión $\sqrt{-(p, -q, r)}$; pero para brevedad no daremos los detalles de esta simplificación. También podemos utilizar estas simplificaciones cuando queremos todas las representaciones propias de M por $x^2 + y^2 + z^2$, puesto que esto se puede obtener muy fácilmente a partir de las descomposiciones.

Como ejemplo investigaremos todas las descomposiciones del número 770 en tres cuadrados. Aquí $\mu = 3$, $e = e' = 0$ y así $E = 2k$. Puesto que es fácil utilizar las normas del artículo 231 para clasificar las formas binarias positivas de determinante -770, omitiremos esta operación para brevedad. Encontramos que el número de clases positivas es $= 32$. Todas ellas son propiamente primitivas y están distribuidas entre ocho géneros de modo que $k = 4$ y $E = 8$. El género cuyo número característico es -1 claramente tiene los caracteres particulares $R5$; $N7$; $N11$ con respecto a los números 5, 7 y 11, y por el artículo 263 concluimos que su carácter respecto al número 8 debe ser 1 y 3, 8. Ahora, en el género con carácter 1 y 3, 8; $R5$; $N7$; $N11$ encontramos cuatro clases. De ellas escogemos las siguientes como representantes $(6, 2, 129)$, $(6, -2, 129)$, $(19, 3, 41)$, $(19, -3, 41)$ y rechazamos la segunda y cuarta puesto que son opuestos de la primera y tercera. En el artículo 289 dimos cuatro descomposiciones de la forma $(19, 3, 41)$. A partir de éstas obtenemos las descomposiciones del número 770 en $9 + 361 + 400$; $16 + 25 + 729$, $81 + 400 + 289$, $576 + 169 + 25$. Similarmente podemos encontrar cuatro descomposiciones de la forma $6t^2 + 4tu + 129u^2$ en

$$(t - 8u)^2 + (2t + u)^2 + (t + 8u)^2, \qquad (t - 10u)^2 + (2t + 5u)^2 + (t + 2u)^2$$
$$(2t - 5u)^2 + (t + 10u)^2 + (t + 2u)^2, \qquad (2t + 7u)^2 + (t - 8u)^2 + (t - 4u)^2$$

Estos provienen directamente de los valores $(48, 369)$, $(62, -149)$, $(92, -159)$, $(202, 61)$ de la expresión $\sqrt{-(6, -2, 129)}$. Como resultado tenemos la descomposición del número 770 en $225 + 256 + 289$, $1 + 144 + 625$, $64 + 81 + 625$, $16 + 225 + 529$. Y no hay descomposiciones fuera de estas ocho.

En cuanto a la descomposición de números en tres cuadrados que tienen divisores comunes, se sigue tan fácilmente a partir del teorema general del artículo 281 que no hace falta recordarlo aquí.

Demostración de los Teoremas de Fermat: todo entero puede descomponerse en tres números triangulares o cuatro cuadrados.

293.

Los argumentos anteriores también proveen una demostración de aquel famoso teorema: *cualquier entero positivo puede descomponerse en tres números triangulares* que fue descubierto por Fermat, pero cuya prueba rigurosa se deseaba hasta ahora. Es claro que cualquier descomposición del número M en números triangulares

$$\frac{1}{2}x(x+1) + \frac{1}{2}y(y+1) + \frac{1}{2}z(z+1)$$

producirá la descomposición del número $8M + 3$ en tres cuadrados impares

$$(2x+1)^2 + (2y+1)^2 + (2z+1)^2$$

y vice versa. Por la teoría anterior, cualquier entero positivo $8M+3$ se puede resolver en tres cuadrados que necesariamente serán impares (ver nota del artículo 291); y el número de resoluciones depende tanto del número de factores primos de $8M + 3$ como del número de clases entre las cuales están distribuidas las formas binarias de determinante $-(8M + 3)$. Habrá el mismo número de descomposiciones del número M en tres números triangulares. Sin embargo, hemos supuesto que para cualquier valor entero de x el número $\frac{1}{2}x(x+1)$ se ve como un número triangular; y si preferimos excluir al cero el teorema debe cambiarse como sigue: Cualquier entero positivo es o triangular o resoluble en dos o tres números triangulares. Un cambio similar se tendría que realizar en el siguiente teorema si quisiéramos excluir al cero como un cuadrado.

A partir de los mismos principios se demuestra otro teorema de Fermat que dice que *cualquier entero positivo se puede descomponer en cuatro cuadrados.* Si

restamos de un número de la forma $4n+2$ cualquier cuadrado (menor que el número), de un número de la forma $4n+1$ un cuadrado par, de un número de la forma $4n+3$ un cuadrado impar, el residuo en todos estos casos será resoluble en tres cuadrados, y el número dado, por lo tanto, en cuatro. Finalmente, un número de la forma $4n$ puede representarse como $4^{\mu}N$ de tal manera que N pertenezca a una de las tres formas anteriores; y cuando N está resuelto en cuatro cuadrados, $4^{\mu}N$ será también resoluble. Podríamos también remover de un número de la forma $8n+3$ el cuadrado de un raíz $\equiv 0 \pmod 4$, de un número de la forma $8n+7$ el cuadrado de un raíz $\equiv 2 \pmod 4$, de un número de la forma $8n+4$ un cuadrado impar y el residuo será resoluble en tres cuadrados. Pero este teorema ya ha sido probado por el ilustre Lagrange, *Nouv. Mém. de l'Ac. de Berlin*, 1770, *p.* 123. Y el ilustre Euler lo explicó mucho más completamente (de manera diferente de la nuestra) en *Acta Ac. Petr.* II, *p.* 48. Hay otros teoremas de Fermat que son como continuaciones de los anteriores. Dicen que cualquier entero es resoluble en cinco números pentagonales, seis hexagonales, siete heptagonales, etc. Pero aún les hace falta la prueba y parecen necesitar principios distintos para su resolución.

Solución de la ecuación $ax^2 + by^2 + cz^2 = 0$.

294.

TEOREMA. *Si los números a, b y c son primos relativos y ninguno* $= 0$ *ni es divisible por un cuadrado, la ecuación*

$$ax^2 + by^2 + cz^2 = 0 \ldots (\Omega)$$

no se puede resolver con enteros (excepto cuando $x = y = z = 0$*, lo cual no vamos a considerar), a menos que* $-bc$*,* $-ac$ *y* $-ab$ *respectivamente sean residuos cuadráticos de a, b y c y estos números tengan signos diferentes; pero cuando estas cuatro condiciones se cumplen,* (Ω) *se podrá resolver con enteros.*

Demostración. Si (Ω) es realmente resoluble por enteros, será también resoluble por valores de x, y y z que no tienen un divisor común; pues cualesquiera valores que satisfacen la ecuación (Ω) también la satisfarán si se dividen por su máximo común divisor. Ahora supongamos que $ap^2 + bq^2 + cr^2 = 0$ y que p, q y r no tienen un divisor común, también serán primos relativos dos a dos, pues si q y r tuvieran un divisor común μ, sería primo relativo a p, pero μ^2 dividiría a ap^2 y así también a a, contrario a la hipótesis, similarmente p, r; p, q deben ser primos relativos. Por esto

$-ap^2$ se representa por una forma binaria $by^2 + cz^2$ asignando a y y z los valores q y r, primos relativos; así su determinante $-bc$ será un residuo cuadrático de ap^2 y así también de a (art. 154); de la misma manera tendremos $-acRb$, $-abRc$. En cuanto a la condición de que (Ω) no admite una resolución si a, b y c tienen el mismo signo, es tan obvio que no necesita una explicación.

Para demostrar la proposición inversa que constituye la segunda parte del teorema, mostraremos *primero*, cómo encontrar una forma ternaria que sea equivalente a $\left(\begin{smallmatrix} a, & b, & c \\ 0, & 0, & 0 \end{smallmatrix}\right) \ldots f$ y escogida tal que los coeficientes segundo, tercero y cuarto sean divisibles por abc; y *segundo*, deduciremos una solución de la ecuación (Ω) a partir de esto.

I. Se buscan tres enteros A, B y C que no tengan un divisor común y escogidos de tal manera que A sea primo relativo a b y c; B sea primo relativo a a y c y C primo relativo a a y b. Entonces $aA^2 + bB^2 + cC^2$ será divisible por abc según se ve de lo siguiente. Sean $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$ respectivamente valores de las expresiones $\sqrt{-bc} \pmod{a}$, $\sqrt{-ac} \pmod{b}$ y $\sqrt{-ab} \pmod{c}$ que necesariamente serán primos relativos a a, b y c respectivamente. Ahora escoja tres enteros arbitrarios $\mathfrak{a}, \mathfrak{b}$ y $\mathfrak{c}$ con la única condición de que sean primos relativos a a, b y c respectivamente (e.g. sean todos $= 1$) y determine A, B y C tales que

$$\begin{aligned} A &\equiv \mathfrak{b}c \pmod{b} \quad \text{y} \quad \equiv \mathfrak{c}\mathfrak{C} \pmod{c} \\ B &\equiv \mathfrak{c}a \pmod{c} \quad \text{y} \quad \equiv \mathfrak{a}\mathfrak{A} \pmod{a} \\ C &\equiv \mathfrak{a}b \pmod{a} \quad \text{y} \quad \equiv \mathfrak{b}\mathfrak{B} \pmod{b} \end{aligned}$$

Entonces resulta

$$aA^2 + bB^2 + cC^2 \equiv \mathfrak{a}^2(b\mathfrak{A}^2 + cb^2) \equiv \mathfrak{a}^2(b\mathfrak{A}^2 - \mathfrak{A}^2 b) \equiv 0 \pmod{a}$$

Así será divisible por a y similarmente por b y por c y también por abc . Además es evidente que A necesariamente es primo relativo a b y c; B a a y c; y C a a y b. Ahora, si los valores A, B y C resultan tener un (máximo) común divisor μ, éste necesariamente será primo relativo a a, b y c, y también a abc; por lo tanto si dividimos estos valores por μ obtendremos nuevos valores que no tienen un divisor común y que producirán un valor de $aA^2 + bB^2 + cC^2$ que aún será divisible por abc, y así satisface a todas las condiciones.

II. Si determinamos los números A, B y C de esta manera, los números Aa, Bb y Cc tampoco tendrán un divisor común. Pues si tuvieran un divisor común μ,

necesariamente tendría que ser primo relativo a a (el cual, de hecho, es primo relativo a Bb y Cc) y similarmente a b y c; por lo tanto μ también tendría que ser divisor de A, B y C contrario a la hipótesis. Por lo tanto podrán encontrarse enteros α, β y γ tales que $\alpha Aa + \beta Bb + \gamma Cc = 1$. Además, búsquense seis enteros α', β', γ', α'', β'' y γ'' tales que

$$\beta'\gamma'' - \gamma'\beta'' = Aa, \qquad \gamma'\alpha'' - \alpha'\gamma'' = Bb, \qquad \alpha'\beta'' - \beta'\alpha'' = Cc$$

Ahora f se transformará por la sustitución

$$\begin{matrix} \alpha, & \alpha', & \alpha'' \\ \beta, & \beta', & \beta'' \\ \gamma, & \gamma', & \gamma'' \end{matrix}$$

en $\left(\begin{smallmatrix} m, & m', & m'' \\ n, & n', & n'' \end{smallmatrix}\right) = g$ (que será equivalente a f) y digo que m', m'' y n serán divisibles por abc. Pues, sea

$$\begin{aligned} \beta''\gamma - \gamma''\beta = A', \qquad & \gamma''\alpha - \alpha''\gamma = B', \qquad & \alpha''\beta - \beta''\alpha = C' \\ \beta\gamma' - \gamma\beta' = A'', \qquad & \gamma\alpha' - \alpha\gamma' = B'', \qquad & \alpha\beta' - \beta\alpha' = C'' \end{aligned}$$

y tendremos

$$\begin{aligned} \alpha' = B''Cc - C''Bb, \qquad & \beta' = C''Aa - A''Cc, \qquad & \gamma' = A''Bb - B''Aa \\ \alpha'' = C'Bb - B'Cc, \qquad & \beta'' = A'Cc - C'Aa, \qquad & \gamma'' = B'Aa - A'Bb \end{aligned}$$

Si sustituimos estos valores en las ecuaciones

$$\begin{aligned} m' &= a\alpha'^2 + b\beta'^2 + c\gamma'^2 \\ m'' &= a\alpha''^2 + b\beta''^2 + c\gamma''^2 \\ n &= a\alpha'\alpha'' + b\beta'\beta'' + c\gamma'\gamma'' \end{aligned}$$

tenemos, según el módulo a

$$\begin{aligned} m' &\equiv bcA''^2(B^2b + C^2c) \equiv 0 \\ m'' &\equiv bcA'^2(B^2b + C^2c) \equiv 0 \\ n &\equiv bcA'A''(B^2b + C^2c) \equiv 0 \end{aligned}$$

i.e. m', m'' y n serán divisibles por a; de manera similar se muestra que los mismos números son divisibles por b y por c y así que son divisibles por abc *Q. E. P.*

III. Pongamos, por razones de elegancia, d igual al determinante de las formas f y g, i.e. el número $-abc$. Entonces

$$md = M, \quad m' = M'd, \quad m'' = M''d, \quad n = Nd, \quad n' = N', \quad n'' = N''$$

Está claro que f se transforma por la sustitución (S)

$$\begin{matrix} \alpha d, & \alpha', & \alpha'' \\ \beta d, & \beta', & \beta'' \\ \gamma d, & \gamma', & \gamma'' \end{matrix}$$

en la forma ternaria $\left(\begin{smallmatrix} Md, & M'd, & M''d \\ Nd, & N'd, & N''d \end{smallmatrix}\right) = g'$ de determinante d^3 que por lo tanto estará contenida en f. Ahora digo que la forma $\left(\begin{smallmatrix} d, & 0, & 0 \\ d, & 0, & 0 \end{smallmatrix}\right) = g''$ es necesariamente equivalente a g'. Pues es claro que $\left(\begin{smallmatrix} M, & M', & M'' \\ N, & N', & N'' \end{smallmatrix}\right) = g'''$ es una forma ternaria de determinante 1; además, puesto que por hipótesis a, b y c no pueden tener el mismo signo, f será una forma indefinida y fácilmente se concluye que g' y g'' también deben ser indefinidas; por lo tanto g''' será equivalente a la forma $\left(\begin{smallmatrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{smallmatrix}\right)$ (art. 277), y se podrá encontrar una transformación (S') de g''' en sí misma; es claro sin embargo que (S') dará una transformación de g' en g''. Por lo tanto g'' también estará contenida en f y mediante una combinación de las sustituciones (S) y (S') se deduce una transformación de f en g''. Si esta transformación es

$$\begin{matrix} \delta, & \delta', & \delta'' \\ \varepsilon, & \varepsilon', & \varepsilon'' \\ \zeta, & \zeta', & \zeta'' \end{matrix}$$

claramente tenemos una doble solución de la ecuación (Ω), a saber $x = \delta'$, $y = \varepsilon'$, $z = \zeta'$ y $x = \delta''$, $y = \varepsilon''$, $z = \zeta''$; de manera similar es claro que no todos estos valores pueden ser $= 0$ a la vez, puesto que debemos tener

$$\delta\varepsilon'\zeta'' + \delta'\varepsilon''\zeta + \delta''\varepsilon\zeta' - \delta\varepsilon''\zeta' - \delta'\varepsilon\zeta'' - \delta''\varepsilon'\zeta = d \quad Q.\ E.\ S.$$

Ejemplo. Sea $7x^2 - 15y^2 + 23z^2 = 0$ la ecuación propuesta. Es resoluble porque $345R7$, $-161R15$, $105R23$. Aquí los valores $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$ serán 3, 7 y 6;

haciendo $\mathfrak{a} = \mathfrak{b} = \mathfrak{c} = 1$ encontramos que $A = 98$, $B = -39$ y $C = -8$. De esto obtenemos la sustitución $\left\{\begin{matrix} 3, & 5, & 22 \\ -1, & 2, & -28 \\ 8, & 25, & -7 \end{matrix}\right\}$ mediante la cual f se transforma en $\left(\begin{matrix} 1520, & 14490, & -7245 \\ -2415, & -1246, & 4735 \end{matrix}\right) = g$. Y como resultado tenemos

$$(S) = \left\{\begin{matrix} 7245, & 5, & 22 \\ -2415, & 2, & -28 \\ 19320, & 25, & -7 \end{matrix}\right\}, \quad g''' = \begin{pmatrix} 3670800, & 6, & -3 \\ & -1, -1246, & 4735 \end{pmatrix}$$

La forma g''' se transforma en $\left(\begin{matrix} 1, & 0, & 0 \\ 1, & 0, & 0 \end{matrix}\right)$ mediante la sustitución

$$\left\{\begin{matrix} 3, & 5, & 1 \\ -2440, & -4066, & -813 \\ -433, & -722, & -144 \end{matrix}\right\} \ldots (S')$$

Si combinamos esto con (S) obtenemos:

$$\left\{\begin{matrix} 9, & 11, & 12 \\ -1, & 9, & -9 \\ -9, & 4, & 3 \end{matrix}\right\}$$

que transformará f en g''. Tenemos entonces una solución doble de la ecuación propuesta $x = 11$, $y = 9$, $z = 4$ y $x = 12$, $y = -9$, $z = 3$; la segunda solución se simplifica dividiéndola por su divisor común 3 y tenemos $x = 4$, $y = -3$, $z = 1$.

295.

La segunda parte del teorema de la sección anterior también se puede resolver como sigue. Se busca un entero h tal que $ah \equiv \mathfrak{C} \pmod{c}$ (le asignamos los mismos significados a los caracteres $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$, que en el artículo anterior) y resulta $ah^2 + b = ci$. Es fácil ver que i es un entero y que $-ab$ es el determinante de la forma binaria $(ac, ah, i) \ldots \varphi$. Ciertamente esta forma no será positiva (puesto que como por hipótesis a, b y c no tienen el mismo signo, ab y ac no pueden ser positivos simultáneamente); además tendrá el número característico -1, que mostramos sintéticamente como sigue. Determine los enteros e y e' tales que

$$e \equiv 0 \pmod{a} \text{ y } \equiv \mathfrak{B} \pmod{b}; \quad ce' \equiv \mathfrak{A} \pmod{a} \text{ y } \equiv h\mathfrak{B} \pmod{b}$$

y (e, e') será un valor de la expresión $\sqrt{-(ac, ah, i)}$ (mod. $-ab$). Pues según el módulo a tenemos

$$e^2 \equiv 0 \equiv -ac, \qquad ee' \equiv 0 \equiv -ah$$
$$c^2 e'^2 \equiv \mathfrak{A}^2 \equiv -bc \equiv -c^2 i \quad \text{entonces} \quad e'^2 \equiv -i$$

y según el módulo b tenemos

$$e^2 \equiv \mathfrak{B}^2 \equiv -ac, \qquad cee' \equiv h\mathfrak{B}^2 \equiv -ach \quad \text{entonces} \quad ee' \equiv -ah$$
$$c^2 e'^2 \equiv h^2 \mathfrak{B}^2 \equiv -ach^2 \equiv -c^2 i \quad \text{entonces} \quad e'^2 \equiv -i$$

y las mismas tres congruencias que son válidas según cada uno de los módulos a y b por separado también serán válidos según el módulo ab. Entonces, por el teorema de formas ternarias, es fácil concluir que φ es representable por la forma $\left(\begin{smallmatrix} -1, 0, 0 \\ 1, 0, 0 \end{smallmatrix}\right)$. Suponga entonces que

$$act^2 + 2ahtu + iu^2 = -(\alpha t + \beta u)^2 + 2(\gamma t + \delta u)(\varepsilon t + \zeta u)$$

Multiplicando por c obtenemos

$$a(ct + hu)^2 + bu^2 = -c(\alpha t + \beta u)^2 + 2c(\gamma t + \delta u)(\varepsilon t + \zeta u)$$

Ahora si le damos a t y u valores tales que ó $\gamma t + \delta u$ ó $\varepsilon t + \zeta u$ sea $= 0$, habrá una solución de la ecuación (Ω) que será satisfecha por

$$x = \delta c - \gamma h, \quad y = \gamma, \quad z = \alpha\delta - \beta\gamma$$

y por

$$x = \zeta c - \varepsilon h, \quad y = \varepsilon, \quad z = \alpha\zeta - \beta\varepsilon$$

Es evidente que no todos los valores en cualquiera de los dos conjuntos puede ser $= 0$ simultáneamente, pues si $\delta c - \gamma h = 0$, $\gamma = 0$, tendríamos también $\delta = 0$ y $\varphi = -(\alpha t + \beta u)^2$, resultando $ab = 0$, contrario a la hipótesis y similarmente para los otros valores. En nuestro ejemplo encontramos que la forma φ es $(161, -63, 24)$, que el valor de la expresión $\sqrt{-\varphi}$ (mod. 105) $= (7, -51)$, y que la representación de la forma φ por $\left(\begin{smallmatrix} -1, 0, 0 \\ 1, 0, 0 \end{smallmatrix}\right)$ es

$$\varphi = -(13t - 4u)^2 + 2(11t - 4u)(15t - 5u)$$

Esto nos da las soluciones $x = 7$, $y = 11$, $z = -8$; $x = 20$, $y = 15$, $z = -5$, o dividiendo por 5 e ignorando el signo de z, $x = 4$, $y = 3$, $z = 1$.

De los dos métodos para resolver la ecuación (Ω), el segundo es preferible porque utiliza números pequeños con más frecuencia; el primero, sin embargo, que puede acortarse mediante varios artificios que omitiremos aquí, parece ser más elegante, especialmente porque los números a, b y c se tratan de la misma manera y los cálculos no se alteran al permutarlos. Por otra parte, es en el segundo método donde tenemos los cálculos más convenientes si dejamos que a sea el menor y c el mayor de los tres números, como hicimos en nuestro ejemplo.

Sobre el método con el cual Legendre trató de demostrar su teorema fundamental.

296.

El elegante teorema que hemos explicado en los artículos anteriores fue descubierto por primera vez por el ilustre Legendre, *Hist. de l'Ac. de Paris*, 1785, *p.* 507, y lo justificó con una demostración bella (enteramente diferente de las dos nuestras). A la vez este geómetra sobresaliente trató de obtener a partir de ello una demostración de proposiciones que se ajustan al teorema fundamental de la sección anterior, pero ya hemos dicho en el artículo 151 que parecía no ser apropiado para este propósito. Entonces, éste es el lugar para explicar esta demostración (extremadamente elegante en sí) de manera breve y dar las razones de nuestra opinión. Empezamos con la siguiente observación: *si los números a, b y c, son todos* $\equiv 1$ (mod. 4)*, la ecuación* $ax^2 + by^2 + cz^2 = 0 \ldots (\Omega)$ *no es resoluble.* En efecto, es fácil ver que en este caso el valor de $ax^2 + by^2 + cz^2$ necesariamente será ó $\equiv 1$, ó $\equiv 2$, ó $\equiv 3$ (mod. 4), excepto si todos los x, y y z son pares a la vez; por lo tanto, si Ω fuera soluble, esto no podría suceder excepto por valores pares de x, y y z, *Q. E. A.*, puesto que cualesquiera que sean los valores que satisfacen la ecuación Ω la seguirán satisfaciendo al dividirse por su máximo común divisor, así que por lo menos uno de los valores debe ser impar. Ahora se obtienen los diferentes casos del teorema por demostrar mediante las consideraciones siguientes.

I. Si p y q son números primos (diferentes y positivos) de la forma $4n + 3$, no podemos tener pRq y qRp a la vez. En efecto, si fuera posible, claramente al poner que $1 = a$, $-p = b$, $-q = c$, todas las condiciones para resolver la ecuación $ax^2 + by^2 + cz^2 = 0$ se cumplirán (art. 294); pero mediante la observación anterior, esta ecuación no tiene solución; por lo tanto, nuestra suposición es inconsistente. De esto sigue inmediatamente la proposición 7 del artículo 131.

II. Si p es un número primo de la forma $4n+1$ y q es un número primo de la forma $4n+3$, no se puede tener simultáneamente qRp y pNq. En efecto, tendríamos $-pRq$ y la ecuación $x^2 + py^2 - qz^2 = 0$ sería resoluble. De esto obtenemos los casos 4 y 5 del artículo 131.

III. Si p y q son números primos de la forma $4n + 1$, no se puede tener simultáneamente pRq y qNp. Sea r otro número primo de la forma $4n+3$ que sea un residuo de q y del cual p sea un no residuo. Entonces por los casos (II) ya demostrados tendremos qRr y rNp. Por lo tanto, si tenemos pRq y qNp tendríamos $qrRp$, $prRq$, $pqNr$ y luego $-pqRr$. Esto haría que la ecuación $px^2 + qy^2 - rz^2 = 0$ fuera resoluble, contrario a la observación anterior; y la suposición sería inconsistente. De esto siguen los casos 1 y 2 del artículo 131.

Este caso se puede tratar más elegantemente de la siguiente manera. Sea r un número primo de la forma $4n+3$ para el cual p sea un no residuo. Entonces tendremos rNp y por lo tanto (suponiendo pRq, qNp) $qrRp$; además, tenemos $-pRq$, $-pRr$, y así también $-pRqr$ y la ecuación $x^2 + py^2 - qrz^2 = 0$ sería resoluble contrario a la observación anterior, etc.

IV. Si p es un número primo de la forma $4n + 1$ y q un primo de la forma $4n + 3$, no se puede tener pRq y qNp simultáneamente. Sea r un número primo auxiliar de la forma $4n+1$ que es un no residuo de ambos p y q. Entonces tendremos (por II) qNr y (por III) pNr; por lo tanto $pqRr$; por lo tanto si pRq, qNp también tendríamos $prNq$, $-prRq$, $qrRp$; así pues la ecuación $px^2 - qy^2 + rz^2 = 0$ sería resoluble, *Q. E. A.* De esto obtenemos los casos 3 y 6 del artículo 131.

V. Si p y q son números primos de la forma $4n + 3$, no podemos tener pNq y qNp simultáneamente. En efecto, si se supone que esto es posible y se toma un número primo auxiliar r de la forma $4n + 1$ que sea un no residuo de ambos p y q, tendremos $qrRp$, $prRq$; además (por II) pNr, qNr y por lo tanto $pqRr$ y $-pqRr$; así que la ecuación $-px^2 - qy^2 + rz^2 = 0$ es posible, contrario a la observación anterior. De esto obtenemos el caso 8 del artículo 131.

297.

Examinando cuidadosamente la demostración anterior cualquier persona puede ver fácilmente que los casos I y II son totalmente completos, de modo que nadie puede objetarlos. Pero las demostraciones de los casos restantes se apoyan en la existencia de números auxiliares, y puesto que su existencia hasta el momento no se ha comprobado, el método claramente pierde toda su fuerza. Aunque estas

suposiciones son tan aparentes que parecen no requerir una demostración, y aunque ciertamente dan el más alto grado de *probabilidad* al teorema que estamos tratando de demostrar, no obstante, si queremos rigor geométrico no podemos simplemente aceptarlas de manera gratuita. En cuanto a la suposición en IV y V de que existe un número primo r de la forma $4n+1$ que es un no residuo de los otros primos dados p y q, es fácil concluir de la Sección IV que todos los números menores que $4pq$ y primos relativos con él (su número es $2(p-1)(q-1)$) se pueden distribuir equitativamente en cuatro clases. Una de ellas contendrá los no residuos de p y q y las tres restantes los residuos de p que son no residuos de q, los no residuos de p que son residuos de q y los residuos de ambos p y q; y en cada clase la mitad de los números serán de la forma $4n+1$ y la otra mitad de la forma $4n+3$. Entre ellos por lo tanto habrá $\frac{1}{4}(p-1)(q-1)$ que son no residuos de p y q de la forma $4n+1$. Los designaremos por g, g', g'', etc., y los restantes $\frac{7}{4}(p-1)(q-1)$ números por h, h', h'', etc. Todos los números contenidos en las formas $4pqt+g$, $4pqt+g'$, $4pqt+g''$, etc. $\ldots(G)$ también serán no residuos de p y q de la forma $4n+1$. Ahora está claro que para establecer nuestra suposición es necesario solamente establecer que las formas (G) contienen *números primos*. Y esto parece ser muy plausible puesto que estas formas junto con las formas $4pqt+h$, $4pqt+h'$, etc. $\ldots(H)$ contienen todos los números que son primos relativos a $4pq$ y son por lo tanto todos números primos absolutos (excepto 2, p y q); y no hay razón por la cual pensar que esta serie de números primos no sea distribuida equitativamente entre las formas de modo que un octavo pertenezca a (G) y el resto a (H). Pero obviamente este razonamiento está lejos del rigor geométrico. El ilustre Legendre mismo confesó que la demostración de un teorema que asegura que números primos ciertamente están contenidos en una forma $kt+l$ (donde k y l son números primos relativos dados y t indefinido) es bastante difícil y sugiere un método que puede ser útil. Nos parece que son necesarias muchas investigaciones preliminares antes de poder llegar a una demostración rigurosa por este camino. En cuanto a la otra suposición (III, segundo método) de que existe un número primo r de la forma $4n+3$ del cual otro número primo dado p de la forma $4n+1$ sea un no residuo, Legendre no agrega nada. Hemos mostrado anteriormente (art. 129) que ciertamente hay números primos para los cuales p es un no residuo, pero nuestro método no parece idóneo para mostrar que existen tales números primos *que sean además de la forma* $4n+3$ (como se requiere aquí pero no en nuestra primera demostración). Sin embargo, podemos probar fácilmente la validez de esta proposición como sigue. Por el artículo 287 existe un género positivo de formas binarias de determinante $-p$ cuyo carácter es 3,4; Np. Sea (a,b,c) tal forma y a impar (esto es permitido). Entonces a será de

la forma $4n + 3$ y primo en sí o al menos divisible por un factor primo r de la forma $4n + 3$. Sin embargo, tenemos $-pRa$ y así también $-pRr$ y como resultado pNr. Pero debemos notar cuidadosamente que las proposiciones de los artículos 263 y 287 dependen del teorema fundamental, y así tendríamos un círculo vicioso si basaramos alguna parte de esta discución en ellos. Finalmente, la suposición del primer método en III es tanto más gratuita que no hay razón por la cual añadir más sobre ella aquí.

Agreguemos una observación sobre el caso V que verdaderamente no ha quedado suficientemente comprobado por el método anterior; sin embargo será resuelto satisfactoriamente por lo que sigue. Si pNq y qNp fueran verdaderos simultáneamente, tendríamos $-pRq$ y $-qRp$, y es fácil verificar que -1 es un número característico de la forma $(p, 0, q)$ que podría entonces (según la teoría de formas ternarias) ser representada por la forma $x^2 + y^2 + z^2$. Sea

$$pt^2 + qu^2 = (\alpha t + \beta u)^2 + (\alpha' t + \beta' u)^2 + (\alpha'' t + \beta'' u)^2$$

o

$$\alpha^2 + \alpha'^2 + \alpha''^2 = p, \qquad \beta^2 + \beta'^2 + \beta''^2 = q, \qquad \alpha\beta + \alpha'\beta' + \alpha''\beta'' = 0$$

y tendremos de las ecuaciones 1 y 2 que todos los números α, α', α'', β, β' y β'' son impares; pero entonces la tercera ecuación no puede ser consistente. El caso II se puede resolver de una manera similar a ésta.

298.

PROBLEMA. *Dados tres números cualesquiera a, b y c diferentes de cero; encontrar las condiciones para la solubilidad de la ecuación*

$$ax^2 + by^2 + cz^2 = 0 \ldots (\omega)$$

Solución. Sean α^2, β^2 y γ^2 los máximos divisores cuadrados de bc, ac y ab respectivamente y sea $\alpha a = \beta\gamma A$, $\beta b = \alpha\gamma B$, $\gamma c = \alpha\beta C$. Entonces A, B y C serán enteros primos relativos entre sí; la ecuación (ω) será resoluble o no según

$$AX^2 + BY^2 + CZ^2 = 0 \ldots (\Omega)$$

admita o no una solución de acuerdo con las normas del artículo 294.

Demostración. Sean $bc = \mathfrak{A}\alpha^2$, $ac = \mathfrak{B}\beta^2, ab = \mathfrak{C}\gamma^2$. $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$ serán enteros libres de factores cuadrados y $\mathfrak{A} = BC$, $\mathfrak{B} = AC$, $\mathfrak{C} = AB$; como resultado $\mathfrak{ABC} = (ABC)^2$ y así $ABC = A\mathfrak{A} = B\mathfrak{B} = C\mathfrak{C}$ es necesariamente un entero. Sea m el máximo común divisor de los números $\mathfrak{A}$ y $A\mathfrak{A}$. Entonces $\mathfrak{A} = gm$, $A\mathfrak{A} = hm$ y g será primo relativo a h y (puesto que $\mathfrak{A}$ está libre de factores cuadrados) a m. Ahora tenemos $h^2m = gA^2\mathfrak{A} = g\mathfrak{BC}$ así que g divide a h^2m, lo cual es obviamente imposible a menos que $g = \pm 1$. Así $\mathfrak{A} = \pm m$, $A = \pm h$ y por lo tanto son enteros y como consecuencia B y C también serán enteros. *Q. E. P.* Puesto que $\mathfrak{A} = BC$ no tiene factores cuadrados, B y C deben ser primos relativos; y similarmente, A será primo relativo a C y a B. *Q. E. S.* Finalmente si $X = P$, $Y = Q$, $Z = R$ satisfacen la ecuación (Ω), la ecuación (ω) será satisfecha por $x = \alpha P$, $y = \beta Q$, $z = \gamma R$; en cambio si (ω) es satisfecha por $x = p$, $y = q$, $z = r$, (Ω) será satisfecha por $X = \beta\gamma p$, $Y = \alpha\gamma q$, $Z = \alpha\beta r$ y así si una es resoluble lo será también la otra. *Q. E. T.*

Representaciones de cero por formas ternarias cualesquiera

299.

PROBLEMA. *Dada la forma ternaria*

$$f = ax^2 + a'x'^2 + a''x''^2 + 2bx'x'' + 2b'xx'' + 2b''xx'$$

determinar si cero es representable por esta forma (sin que todas las incógnitas sean = 0 simultáneamente).

Solución. I. Cuando $a = 0$ los valores de x' y x'', se pueden tomar arbitrariamente y es claro de la ecuación

$$a'x'^2 + 2bx'x'' + a''x''^2 = -2x(b'x'' + b''x')$$

que x tomará un valor racional determinado; cuando obtenemos una fracción como valor de x, sólo debemos multiplicar los valores de x, x' y x'' por el denominador de la fracción para obtener enteros. Los únicos valores de x' y x'' que se deben excluir son aquéllos que hacen que $b'x'' + b''x' = 0$ a menos que también satisfagan $a'x'^2 + 2bx'x'' + a''x''^2 = 0$, en cuyo caso x es arbitrario. Así se pueden obtener todas las posibles soluciones. Pero el caso donde $b' = b'' = 0$ no se contempla aquí pues entonces x no participaría en la determinación de f; esto es, f es una forma binaria y la posible representación de cero por f debe decidirse a partir de la teoría de tales formas.

II. Cuando tenemos $a \neq 0$, la ecuación $f = 0$ será equivalente a

$$(ax + b''x' + b'x'')^2 - A''x'^2 + 2Bx'x'' - A'x''^2 = 0$$

al poner

$$b''^2 - aa' = A'', \qquad ab - b'b'' = B, \qquad b'^2 - aa'' = A'.$$

Ahora, cuando $A' = 0$ y $B \neq 0$ es claro que si tomamos $ax + b''x' + b'x''$ y x'' arbitrariamente, x y x' serán números racionales y cuando no son enteros se pueden hacer enteros mediante una multiplicación apropiada. Para un valor de x'', a saber $x'' = 0$, el valor de $ax + b''x' + b'x''$ no es arbitrario pero debe ser también $= 0$; pero el x' se puede tomar con completa libertad y producirá un valor de x racional. Cuando A'' y $B = 0$ simultáneamente, es claro que si A' es un cuadrado $= k^2$, la ecuación $f = 0$ se reduce a las siguientes dos ecuaciones lineales (donde una u otra debe tener lugar)

$$ax + b''x' + (b' + k)x'' = 0, \qquad ax + b''x' + (b' - k)x'' = 0$$

pero si (bajo la misma hipótesis) A' no es un cuadrado, la solución de la ecuación propuesta depende de las siguientes (ambas deben cumplirse) $x'' = 0$ y $ax + b''x' = 0$.

Será apenas necesario notar que el método de I es aplicable cuando a' o $a'' = 0$ y el método de II cuando $A' = 0$.

III. Cuando ni a ni $A'' = 0$, la ecuación $f = 0$ será equivalente a

$$A''(ax + b''x' + b'x'')^2 - (A''x' - Bx'')^2 + Dax''^2 = 0$$

donde D es el determinante de la forma f y Da es el número $B^2 - A'A''$. Cuando $D = 0$ tendremos una solución como la del final del caso anterior; eso es, si A'' es un cuadrado $= k^2$, la ecuación propuesta se reduce a éstas:

$$kax + (kb'' - A'')x' + (kb' + B)x'' = 0, \qquad kax + (kb'' + A'')x' + (kb'' - B)x'' = 0$$

pero si A'' no es un cuadrado, se debe tener

$$ax + b''x' + b'x'' = 0, \qquad A''x' - Bx'' = 0$$

Sin embargo, cuando D no es $= 0$ se nos reduce a la ecuación

$$A''t^2 - u^2 + Dav^2 = 0$$

una posibilidad que se puede decidir mediante el artículo anterior. Si esta ecuación no se puede resolver excepto para $t = 0$, $u = 0$ y $v = 0$, la ecuación propuesta no admite ninguna solución salvo $x = 0$, $x' = 0$ y $x'' = 0$; pero si tiene como solución cualquier otro conjunto de enteros t, u y v podemos mediante las ecuaciones

$$ax + b''x' + b'x'' = t, \qquad A''x' - Bx'' = u, \qquad x'' = v$$

obtener por lo menos valores racionales de x, x' y x''. Si éstas incluyen fracciones, podemos hacerlas enteros mediante una multiplicación apropiada.

Tan pronto se encuentra *una* solución de la ecuación $f = 0$ por enteros, el problema se reduce al caso I y todas las soluciones se pueden encontrar de la siguiente manera. Sean α, α' y α'' algunos valores de x, x' y x'' que satisfacen la ecuación $f = 0$. Supongamos que no tienen factores comunes. Ahora (por art. 40, 279) escoja enteros β, β', β'', γ, γ' y γ'' tales que

$$\alpha(\beta'\gamma'' - \beta''\gamma') + \alpha'(\beta''\gamma - \beta\gamma'') + \alpha''(\beta\gamma' - \beta'\gamma) = 1$$

y la forma f se transformará, por la sustitución

$$x = \alpha y + \beta y' + \gamma y'', \qquad x' = \alpha' y + \beta' y' + \gamma' y'', \qquad x'' = \alpha'' y + \beta'' y' + \gamma'' y'' \quad (S)$$

en la forma

$$g = cy^2 + c'y'^2 + c''y''^2 + 2dy'y'' + 2d'yy'' + 2d''yy'$$

Entonces se tendrá $c = 0$ y g será equivalente a f, de donde se concluye fácilmente que todas las soluciones por enteros de la ecuación $f = 0$ pueden obtenerse (por S) de todas las soluciones de $g = 0$. Y por I todas las soluciones de la ecuación $g = 0$ están contenidas en las fórmulas

$$y = -z(c'p^2 + 2dpq + c''q^2), \qquad y' = 2z(d''p^2 + d'pq), \qquad y'' = 2z(d''pq + d'q^2)$$

donde p y q son enteros cualesquiera , z un número cualquiera que puede ser una fracción siempre y cuando y, y' e y'' sean enteros. Si sustituimos estos valores de y, y' e y'' en (S), se tendrán todas las soluciones de la ecuación $f = 0$ por enteros. Así, por ejemplo, si

$$f = x^2 + x'^2 + x''^2 - 4x'x'' + 2xx'' + 8xx'$$

y una solución de la ecuación $f = 0$ es $x = 1$, $x' = -2$, $x'' = 1$; haciendo β, β', β'', γ, γ', $\gamma'' = 0$, 1, 0, 0, 0, 1 tenemos

$$g = y'^2 + y''^2 - 4y'y'' + 12yy''$$

Todas las soluciones de la ecuación $g = 0$ por enteros estarán contenidas en la fórmula

$$y = -z(p^2 - 4pq + q^2), \qquad y' = 12zpq, \qquad y'' = 12zq^2$$

y todas las soluciones de la ecuación $f = 0$ en las fórmulas

$$\begin{aligned} x &= -z(p^2 - 4pq + q^2) \\ x' &= 2z(p^2 + 2pq + q^2) \\ x'' &= -z(p^2 - 4pq - 11q^2) \end{aligned}$$

Solución general por racionales de ecuaciones de segundo grado en dos variables.

300.

A partir del problema del artículo anterior se obtiene inmediatamente la solución de la ecuación indeterminada

$$ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0$$

si se buscan sólo valores racionales. Ya la hemos resuelto para valores enteros (art. 216 y siguientes). Todo valor racional de x e y puede representarse por $\frac{t}{v}$ y $\frac{u}{v}$, donde t, u y v son enteros. Así pues, es claro que la solución de esta ecuación por números racionales es idéntica a la solución por enteros de la ecuación

$$at^2 + 2btu + cu^2 + 2dtv + 2euv + fv^2 = 0$$

y esto coincide con la ecuación tratada en el artículo anterior. Excluimos sólo aquellas soluciones donde $v = 0$; pero no puede ocurrir ninguna de este tipo cuando $b^2 - ac$ es un número no cuadrado. Así pues, e.g., toda solución por números racionales de la ecuación (resuelta de modo general por enteros en el art. 221)

$$x^2 + 8xy + y^2 + 2x - 4y + 1 = 0$$

estará contenida en la fórmula

$$x = \frac{p^2 - 4pq + q^2}{p^2 - 4pq - 11q^2}, \qquad y = -\frac{2p^2 + 4pq + 2q^2}{p^2 - 4pq - 11q^2}$$

donde p y q son enteros cualesquiera. Pero aquí hemos tratado brevemente estos dos problemas que están íntimamente conectados dejando por fuera muchas observaciones pertinentes para no hacernos demasiado prolijos. Tenemos otra solución del problema del artículo anterior basada en principios generales, sin embargo se tratará en otra ocasión puesto que requiere de un estudio más profundo de las formas ternarias.

Del número promedio de géneros.

301.

Regresemos ahora al estudio de las formas binarias de las cuales tenemos aún muchas propiedades notables que examinar. Primero le agregaremos algunas observaciones sobre el número de clases y géneros en un orden propiamente primitivo (positivo si el determinante es negativo) y para brevedad restringiremos nuestra investigación a éstas.

El *número de géneros* en los cuales se distribuyen todas las formas (propiamente primitivas positivas) de determinante $\pm D$ positivo o negativo es siempre 1, 2, 4 ó una potencia mayor de 2 cuyo exponente depende de los factores de D y que se puede encontrar a priori mediante el argumento presentado anteriormente. Ahora, puesto que en una serie de números naturales los números primos están mezclados con números más o menos compuestos, sucede que para muchos determinantes sucesivos $\pm D$, $\pm(D+1)$, $\pm(D+2)$, etc. el número de géneros crece y decrece de manera desordenada. Sin embargo, si sumamos los números de géneros correspondientes a muchos determinantes sucesivos

$$\pm D, \quad \pm(D+1), \quad \ldots \pm(D+m)$$

y dividimos la suma por el número de determinantes, obtenemos el *número promedio de géneros*. Se puede considerarlo como si correspondiera al determinante central $\pm(D + \frac{1}{2}m)$ de la serie y establece una progresión muy regular. Supongamos no sólo que m es suficientemente grande sino también que D sea mucho mayor, de modo que la razón de los determinantes extremos D, $D+m$ no difiera mucho de la igualdad. La regularidad de esta progresión debe entenderse así: si D' es un número mucho mayor

que D, el número promedio de determinantes alrededor de D' será notablemente mayor que alrededor de D; y si D y D' no difieren por mucho, el número promedio de géneros alrededor de D y D' será aproximadamente igual. Pero el número promedio de géneros alrededor del determinante positivo $+D$ siempre será aproximadamente igual al número de géneros alrededor del correspondiente determinante negativo y entre mayor sea el valor de D, más cierto será lo anterior mientras que para valores pequeños el número de géneros correspondiente al determinante positivo será un poco mayor que el del determinante negativo. Estas observaciones quedarán ilustradas mejor por los siguientes ejemplos tomados de la tabla que clasifica a las formas binarias para más de 4000 determinantes. Entre los cien determinantes de 801 a 900 hay 7 que corresponden a un único género, 32, 52, 8, 1, que corresponden respectivamente a 2, 4, 8, 16 géneros. Hay en total 359 géneros y un número promedio de 3,59. Los cien determinantes negativos de -801 a -900 producen 360 géneros. Los siguientes ejemplos se toman con determinantes negativos. En la centena 16 (desde -1501 a -1600) el número promedio de géneros es 3,89; en la centena 25 es 4,03; en la centena 51 es 4,24; para los 600 determinantes desde -9401 a -10000 es 4,59. De estos ejemplos es claro que el número promedio de géneros crece mucho más lentamente que los determinantes mismos, pero se busca la ley que describe esta progresión. Mediante una discusión teórica bastante difícil, cuya explicación sería demasiado larga para presentar aquí, se encontró que el número promedio de géneros alrededor de $+D$ o $-D$ puede calcularse aproximadamente por la fórmula

$$\alpha \log D + \beta$$

donde α y β son cantidades constantes y de hecho

$$\alpha = \frac{4}{\pi^2} = 0{,}4052847346$$

(π es la mitad de la circunferencia de un círculo de radio unitario),

$$\beta = 2\alpha g + 3\alpha^2 h - \frac{1}{6} a \log 2 = 0{,}8830460462$$

donde g es el valor de la serie

$$1 - \log(1+1) + \frac{1}{2} - \log(1+\frac{1}{2}) + \frac{1}{3} - \log(1+\frac{1}{3}) + \text{ etc.} = 0{,}5772156649$$

(ver Euler, *Inst. Calc. Diff.* p. 444) y h es el valor de la serie

$$\frac{1}{4}\log 2 + \frac{1}{9}\log 3 + \frac{1}{16}\log 4 + \text{ etc.}$$

que es aproximadamente = 0,9375482543. A partir de esta fórmula es claro que el número promedio de géneros aumenta en una progresión aritmética si los determinantes aumentan en una progresión geométrica. Los valores que nos proporciona esta fórmula para $D = 850\frac{1}{2},\ 1550\frac{1}{2},\ 2450\frac{1}{2},\ 5050\frac{1}{2},\ 9700\frac{1}{2}$ resultan ser 3,617; 3,86; 4,046; 4,339; 4,604; los cuales difieren poco de los valores presentados anteriormente. Entre mayor sea el determinante central y el número de determinantes a partir de los cuales se calcula el promedio, menor será la diferencia entre el valor real y el que se obtiene con la fórmula. Con la ayuda de esta fórmula, también se puede encontrar la suma aproximada del número de géneros que corresponden a determinantes sucesivos $\pm D$, $\pm(D+1)$, $\ldots \pm(D+m)$ sumando el número promedio correspondiente a cada uno sin importar que tan separados estén D y $D+m$. Esta suma será

$$= \alpha\,(\log D + \log(D+1) + \text{ etc.} + \log(D+m)) + \beta(m+1)$$

o con bastante exactitud

$$= \alpha\,((D+m)\log(D+m) - (D-1)\log(D-1)) + (\beta-\alpha)(m+1)$$

De esta manera la suma del número de géneros para los determinantes -1 a -100 resulta ser 234,4, mientras que su valor real es 233; similarmente desde -1 a -2000 la fórmula nos da 7116,6 mientras que el valor real es 7112; de -9001 a -10000 el valor real es 4595 y el aproximado por la fórmula 4594,9, una aproximación mejor de lo que se podría esperar.

Del número promedio de clases.

302.

En cuanto al *número de clases* (siempre asumimos que son propiamente primitivas positivas) los determinantes positivos se comportan de una manera completamente diferente a los determinantes negativos; por lo tanto los consideraremos separadamente. Concuerdan en el hecho de que para un determinante dado hay igual

número de clases en cada género, y por lo tanto el número de clases es igual al producto del número de géneros por el número de clases en cada uno.

Primero, con respecto a los determinantes negativos, el número de clases que corresponde a varios determinantes sucesivos $-D$, $-(D+1)$, $-(D+2)$, etc. genera una progresión que es tan irregular como el número de géneros. El número promedio de clases, sin embargo, (no hace falta una definición) aumenta de manera muy regular como se notará en los siguientes ejemplos. Los cien determinantes de -500 a -600 proporcionan 1729 clases y así el número promedio es 17,29. Similarmente en la centena #15 el número promedio de clases es 28,26; para la #24 y #25 se calcula 36,28; para la #61, #62 y #63 resulta 58,50; para las cinco centenas de #91 a #95 se encuentra 71,56; finalmente para las cinco de 96 a 100 se tiene 73,54. Estos ejemplos muestran que el número promedio de clases crece más lentamente que los determinantes pero mucho más rápidamente que el número promedio de géneros; con una leve atención se puede ver que crece casi exactamente en proporción a la raíz cuadrada del determinante central. De hecho hemos encontrado mediante una investigación teórica que el número promedio de clases cerca del determinante $-D$ se puede expresar aproximadamente como

$$\gamma\sqrt{D} - \delta$$

donde

$$\gamma = 0{,}7467183115 = \frac{2\pi}{7e}$$

donde e es la suma de la serie

$$1 + \frac{1}{8} + \frac{1}{27} + \frac{1}{64} + \frac{1}{125} + \text{ etc.}$$

$$\delta = 0{,}2026423673 = \frac{2}{\pi^2}$$

Los valores promedios obtenidos mediante la fórmula difieren poco de los valores tomados de la tabla de clasificaciones mencionada arriba. Con la ayuda de esta fórmula también se puede aproximar el número de clases (propiamente primitivas positivas) que corresponden a los determinantes sucesivos $-D$, $-(D+1)$, $-(D+2)$, $\ldots -(D+m-1)$, sin importar la separación de los extremos, sumando los números promedios correspondientes a estos determinantes, obtenidos según la fórmula. Se encuentra una suma

$$= \gamma\left(\sqrt{D} + \sqrt{D+1} + \text{ etc.} + \sqrt{D+m-1}\right) - \delta m$$

o aproximadamente

$$= \frac{2}{3}\gamma \left((D+m-\frac{1}{2})^{\frac{3}{2}} - (D-\frac{1}{2})^{\frac{3}{2}} \right) - \delta m$$

Así pues, e.g., por medio de la fórmula la suma de los cien determinantes -1 a -100 será 481,1, mientras que el valor real es 477; los mil determinantes entre -1 y -1000 según la tabla proporcionan 15533 clases, mientras que el valor que nos da la fórmula es 15551,4; en el segundo milenio según la tabla hay 28595 clases, y según la fórmula 28585,7. Similarmente el tercer milenio realmente tiene 37092 clases; la fórmula da 37074,3; el décimo milenio posee 72549 según la tabla y 72572 según la fórmula.

303.

La tabla de determinantes negativos ordenados según varias clasificaciones ofrece muchas otras observaciones notables. Para determinantes de la forma $-(8n+3)$ el número de clases (tanto el número total como el número de clases contenido en cada género propiamente primitivo) es siempre divisible por tres, con la única excepción del determinante -3, como se puede concluir del artículo 256, VI. Para aquellos determinantes cuyas formas están contenidas en un solo género, el número de clases es siempre impar, puesto que para estos determinantes hay una única clase ambigua, la principal, las restantes clases siempre están opuestas en parejas y el número de ellas es por lo tanto par, lo cual hace impar el número total de clases. Esta última propiedad es también válida para determinantes positivos. Además, la serie de determinantes que corresponden a una clasificación dada (i.e. un número dado de géneros y de clases) parece siempre finita e ilustramos esta observación notable con los siguientes ejemplos. (El numeral romano indica el número de géneros propiamente primitivos positivos, el numeral arábigo el número de clases en cada género, luego sigue la serie de determinantes que corresponde a esta clasificación. Por razones de brevedad omitimos el signo negativo.)

I. $1 \ldots 1, 2, 3, 4, 7$

I. $3 \ldots 11, 19, 23, 27, 31, 43, 67, 163$

I. $5 \ldots 47, 79, 103, 127$

I. $7 \ldots 71, 151, 223, 343, 463, 487$

II. $1 \ldots 5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58$

II. $2 \ldots 14, 17, 20, 32, 34, 36, 39, 46, 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193$

IV. $1 \ldots 21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253$

VIII. $1 \ldots 105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760$

XVI. $1 \ldots 840, 1320, 1365, 1848$

Similarmente, se encuentran 20 determinantes (el mayor $= -1423$) que corresponden a la clasificación I. 9; 4 (el mayor $= -1303$) que corresponden a la clasificación I. 11 etc; a las clasificaciones II. 3, II. 4, II. 5, IV. 2, corresponden no más de 48, 31, 44 y 69 determinantes respectivamente, donde los mayores son -652, -862, -1318 y -1012. Puesto que la tabla de la cual obtuvimos estos valores se ha extendido mucho más allá que el mayor determinante que aparece aquí*) y puesto que no proporciona ningún otro que pertenezca a estas clases, no hay duda de que las series anteriores terminan, y por analogía es permitido extender la conclusión a cualquier otra clasificación. Por ejemplo, puesto que en todo el décimo milenio de determinantes, no hay ninguno que corresponde a menos de 24 clases, es muy probable que las clasificaciones I. 23, I. 21, etc. II. 11, II. 10, etc. IV. 5, IV. 4, IV. 3; VIII. 2 están todas completas antes de llegar al número -9000 o que por lo menos tienen muy pocos determinantes mayores que -10000. Sin embargo, probar *rigurosamente* estas observaciones parece ser muy difícil. Es también notable que todo determinante cuyas formas se distribuyen entre 32 o más géneros tiene por lo menos dos clases en cada género y, por lo tanto, que las clasificaciones XXXII. 1, LXIV. 1 etc. no existen del todo (el determinante menor entre éstos es -9240 y corresponde a la clasificación XXXII. 2); y parece ser muy probable que cuando crece el número de géneros más clasificaciones desaparecen. En este aspecto los 65 determinantes mencionados anteriormente, aquéllos de las clasificaciones I. 1, II. 1, IV. 1, VIII. 1, XVI. 1, son bastante excepcionales, y es fácil ver que sólo ellos gozan de dos propiedades notables: todas las clases de las formas que pertenecen a ellos son ambiguas y todas las formas contenidas en el mismo género son a la vez propia e impropiamente equivalentes. El ilustre Euler en *Nouv. Mém. de l'Ac. de Berlin*, 1776, *p.* 338 ya ha determinado estos 65 números (bajo un aspecto ligeramente diferente que mencionaremos luego, y con un criterio que es fácil de demostrar).

*) Mientras esto estaba en impresión calculamos la tabla hasta -3000 *completamente* y también para todo el décimo milenio, para muchas centenas separadas y para muchos determinantes individuales cuidadosamente seleccionados.

304.

El número de clases propiamente primitivas que corresponden a formas binarias con un determinante *cuadrado* positivo k^2 puede determinarse completamente a priori; hay tantas clases como números primos relativos a $2k$ y menores que él. De este hecho y siguiendo un razonamiento fácil, que omitimos aquí, deducimos que el número promedio de clases alrededor de k^2 que pertenecen a tales determinantes es aproximadamente $\frac{8k}{\pi^2}$. Al respecto, sin embargo, determinantes positivos no cuadrados presentan fenómenos singulares. A saber, hay sólo un número pequeño de clases para determinantes pequeños negativos o cuadrados, e.g., clasificación I. 1 ó I. 3 ó II. 1 etc., y la serie termina rápidamente; al contrario, para determinantes positivos no cuadrados, siempre y cuando no sean muy grandes, la gran mayoría de ellos producen clasificaciones en las cuales sólo una clase está contenida en cada género. Así pues, clasificaciones como I. 3, I. 5, II. 2, II. 3, IV. 2, etc. son muy raras. Por ejemplo, entre los 90 determinantes inferiores a 100 encontramos 11, 48 y 27, que corresponden a las clasificaciones I. 1, II. 1, IV. 1 respectivamente; sólo uno (37) tiene I. 3; dos (34 y 82) tienen II. 2; uno (79) tiene II. 3. Sin embargo, al aumentar los determinantes, aparecen números mayores de clases y lo hacen con mayor frecuencia; así pues, entre los 96 determinantes no cuadrados entre 101 y 200, dos (101, 197) tienen la clasificación I. 3; cuatro (145, 146, 178, 194) tienen II. 2; tres (141, 148, 189) tienen II. 3. Entre los 197 determinantes de 801 a 1000, tres tienen I. 3; cuatro II. 2; catorce tienen II. 3; dos tienen II. 5; dos tienen II. 6; quince tienen IV. 2; seis tienen IV. 3; dos tienen IV. 4; cuatro tienen VIII. 2. Los 145 restantes tienen una clase en cada género. Es curioso y sería digno de un geómetra, investigar la ley que justifique el hecho de que los determinantes con una clase por cada género se hacen menos frecuentes. Hasta el momento no podemos asegurar teóricamente ni conjeturar por observación si hay un número finito de ellos (esto es poco probable) o si se hacen *infinitamente raros* o que su frecuencia tiende a un límite fijo. El número promedio de clases aumenta por una razón ligeramente mayor que la razón con que varía el número de géneros y más lentamente que las raíces cuadradas de los determinantes. Entre 800 y 1000 se encuentra $5,01$. Se puede agregar a estas observaciones otra que apoya la analogía entre los determinantes negativos y positivos. Hemos encontrado que para un determinante positivo D, no es el número de clases sino este número multiplicado por el logaritmo de $t + u\sqrt{D}$ (t y u son los números menores, diferentes de 1 y 0, que satisfacen la ecuación $t^2 - Du^2 = 1$) el que es análogo al número de clases para un determinante negativo. No podemos explicar esto más a fondo, pero el valor promedio de ese producto es dado aproximadamente por una fórmula

como $m\sqrt{D} - n$. Pero aun no hemos podido determinar teóricamente los valores de las constantes m y n. Si se permite llegar a una conclusión válida con base en la comparación de unas cuantas centenas, parece que m es aproximadamente $2\frac{1}{3}$. Reservamos para otra ocasión una discusión más completa de los principios detrás de la discusión anterior sobre los valores promedios de cantidades que no siguen una ley analítica, sino que se aproximan asintóticamente a una ley analítica. Pasamos ahora a otra investigación, la comparación de diferentes clases propiamente primitivas de un mismo determinante y así terminará esta larga sección.

Algoritmo singular para clases propiamente primitivas; determinantes regulares, etc.

305.

TEOREMA. *Si K es la clase principal de formas de un determinante dado D, y C es otra clase cualquiera del género principal del mismo determinante; y si $2C$, $3C$, $4C$, etc. son las clases que resultan (como en art. 249) de la duplicación, triplicación, cuadruplicación, etc. de la clase C; entonces si continuamos la progresión C, $2C$, $3C$, etc. lo suficiente, finalmente obtendremos una clase que es idéntica a K; y suponiendo que mC es la primera que es idéntica a K y que el número de clases en el género principal $= n$, entonces tendremos que $m = n$ o que m será un factor de n.*

Demostración. I. Puesto que todas las clases K, C, $2C$, $3C$, etc., necesariamente pertenecen al género principal (art. 247), las primeras $n + 1$ clases de la serie K, C, $2C$, $3C$, $\ldots nC$ no pueden ser todas diferentes. Entonces, K será idéntica a alguna de las clases C, $2C$, $3C$, $\ldots nC$ o al menos dos de ellas serán idénticas entre sí. Sea $rC = sC$ y $r > s$; se tendrá también

$$(r-1)C = (s-1)C, \quad (r-2)C = (s-2)C \text{ etc.} \quad \text{y} \quad (r+1-s)C = C$$

por lo tanto $(r - s)C = K$. *Q. E. P.*

II. También sigue directamente de esto que $m = n$ o que $m < n$, y sólo queda demostrar que en el segundo caso m es un factor de n. Puesto que las clases

$$K,\ C,\ 2C,\ \ldots (m-1)C$$

las cuales designaremos como $\mathfrak{C}$, no agotan el género principal, sea C' una clase de este género que no está contenida en $\mathfrak{C}$. Ahora sea $\mathfrak{C}'$ el conjunto de clases que resulta de la composición de C' con las clases individuales de $\mathfrak{C}$, a saber

$$C', \quad C' + C, \quad C' + 2C, \quad C' + (m-1)C$$

Ahora, obviamente todas las clases en $\mathfrak{C}'$ serán diferentes entre sí, serán diferentes de todas las clases en $\mathfrak{C}$ y pertenecerán al género principal; si $\mathfrak{C}$ y $\mathfrak{C}'$ agotan completamente este género, entonces tendremos $n = 2m$; si no, $2m < n$. En el segundo caso sea C'' cualquier clase del género principal que no está comprendida ni en $\mathfrak{C}$ ni en $\mathfrak{C}'$ y designaremos por $\mathfrak{C}''$ el conjunto de clases que resulta de la composición de la clase C'' con las clases individuales de $\mathfrak{C}$; i.e.

$$C'', \quad C'' + C, \quad C'' + 2C, \quad \dots C'' + (m-1)C$$

y es claro que todas éstas son diferentes entre sí y diferentes de todas las clases en $\mathfrak{C}$ y $\mathfrak{C}'$, y pertenecen al género principal. Ahora, si $\mathfrak{C}$, $\mathfrak{C}'$ y $\mathfrak{C}''$ agotan este género, tendremos que $n = 3m$; si no, $n > 3m$. En este caso hay otra clase C''' del género principal que no está comprendida en $\mathfrak{C}$, $\mathfrak{C}'$, $\mathfrak{C}''$. De manera similar encontramos que $n = 4m$ o $n > 4m$ y así sucesivamente. Ahora puesto que n y m son finitos, el género principal debe agotarse eventualmente y n será un múltiplo de m, o m un factor de n. *Q. E. S.*

Ejemplo. Sea $D = -356$, $C = (5, 2, 72)$*). Se encuentra $2C = (20, 8, 21)$, $3C = (4, 0, 89)$, $4C = (20, -8, 21)$, $5C = (5, -2, 72)$, $6C = (1, 0, 356)$. Aquí $m = 6$ y para este determinante $n = 12$. Si tomamos $(8, 2, 45)$ como la clase C' las restantes cinco clases de $\mathfrak{C}'$ serán $(9, -2, 40)$, $(9, 2, 40)$, $(8, -2, 45)$, $(17, 1, 21)$ y $(17, -1, 21)$.

306.

La demostración del teorema anterior es análoga a las demostraciones en los artículos 45 y 49, y de hecho la teoría de multiplicación de clases es muy afín con el argumento dado en la sección III. Pero las limitaciones de este trabajo no permiten proseguir el tratamiento más profundo que merece esta teoría y sólo agregaremos algunas observaciones, dejando para otra ocasión aquellas demostraciones que requieren mucho detalle.

I. Si la serie K, C, $2C$, $3C$, $\dots$etc. se extiende más allá de $(m-1)C$, obtendremos las mismas clases de nuevo.

$$mC = K, \quad (m+1)C = C, \quad (m+2)C = 2C \quad \text{etc.}$$

*) Siempre expresamos las clases por las *formas* (más sencillas) que contienen.

y en general (tomando K como $0C$), las clases gC y $g'C$ serán idénticas o diferentes según g y g' sean congruentes o no respecto al módulo m. Por lo tanto la clase nC siempre será idéntica a la clase principal K.

II. El conjunto de clases K, C, $2C$, ... $(m-1)C$ que designamos anteriormente como $\mathfrak{C}$ se llamará el *período* de la clase C. Esto no debe confundirse con los *períodos* de *formas* reducidas de un determinante no cuadrado positivo como se trató en el artículo 186 y siguientes. Es claro por lo tanto que la composición de cualquier número de clases contenidas en el mismo período dará una nueva clase que también estará comprendida en el mismo período

$$gC + g'C + g''C \text{ etc.} = (g + g' + g'' + \text{ etc.})C$$

III. Puesto que $C + (m-1)C = K$, las clases C y $(m-1)C$ serán opuestas, así también $2C$ y $(m-2)C$, $3C$ y $(m-3)C$ etc. Por lo tanto, si m es par, la clase $\frac{1}{2}mC$ será opuesta a sí misma y así, *ambigua*; recíprocamente si en $\mathfrak{C}$ aparece alguna clase además de K que sea ambigua, por ejemplo gC, tendremos $gC = (m-g)C$ y así $g = m - g = \frac{1}{2}m$. Se sigue que si m es par no puede haber una clase ambigua en $\mathfrak{C}$ excepto K y $\frac{1}{2}mC$; si m es impar, ninguna excepto K.

IV. Si suponemos que el período de cualquier clase hC contenida en $\mathfrak{C}$ es

$$K, \quad hC, \quad 2hC, \quad 3hC, \quad \ldots (m'-1)hC$$

es claro que $m'h$ es el menor multiplo de h divisible por m. Entonces, si h y m son primos relativos, se tendrá $m' = m$ y ambos períodos contendrán las mismas clases pero en orden diferente. En general, si μ es el máximo común divisor de m y h, será $m' = \frac{m}{\mu}$. Así es claro que el número de clases comprendidas en el período de cualquier clase de $\mathfrak{C}$ será m o un factor de m; de hecho habrá tantas clases en $\mathfrak{C}$ de período m como números en la serie 0, 1, 2, $\ldots m-1$ que son primos relativos a m, o sea φm, utilizando la simbología del artículo 39, y en general, habrá tantas clases en $\mathfrak{C}$ con período $\frac{m}{\mu}$ como números de la serie 0, 1, 2, $\ldots m-1$ que tienen a μ como el máximo común divisor de ellos y m. Es fácil ver que el número de ellas será $\varphi\frac{m}{\mu}$. Si por lo tanto $m = n$ o sea el género principal *completo* está contenido en $\mathfrak{C}$, habrá φn clases en este género cuyos períodos incluyen todo el género y φe clases cuyos períodos son de e términos, donde e es cualquier divisor de n. Esta conclusión es verdadera cuando existe una clase del género principal cuyo período es de n términos.

V. Bajo la misma suposición, la mejor manera de hacer un arreglo de un sistema de clases del género principal es tomar como *base* una clase de período n, colocando las clases del género principal en el mismo orden con el que aparecen en este período. Ahora, si le asignamos el *índice* 0 a la clase principal, 1 a la que tomamos como base y así sucesivamente, entonces con sólo sumar los índices, se puede determinar cual clase resultará de la composición de cualquiera de las clases del género principal. Aquí sigue un ejemplo para el determinante -356, donde tomamos la clase $(9, 2, 40)$ como la base:

0	$(1, \ 0, 356)$	4	$(20, \ 8, 21)$	8	$(20, -8, 21)$
1	$(9, \ 2, \ 40)$	5	$(17, \ 1, 21)$	9	$(\ 8, \ 2, 45)$
2	$(5, \ 2, \ 72)$	6	$(\ 4, \ 0, 89)$	10	$(\ 5, -2, 72)$
3	$(8, -2, \ 45)$	7	$(17, -1, 21)$	11	$(\ 9, -2, 40)$

VI. Aunque tanto una analogía con la sección III como una inducción con más de 200 determinantes negativos y aún más determinantes positivos no cuadrados parecen justificar que la suposición es válida para *todo* determinante, tal conclusión sería falsa y se refutaría por una extensión de la tabla de clasificaciones. Para brevedad llamaremos *regulares* a aquellos determinantes para los cuales el género principal completo puede incluirse en un período, e *irregulares* a aquéllos para los que esto no es posible. Podemos ilustrar con sólo unas pocas observaciones este asunto, el cual depende de los misterios más profundos de la aritmética superior e involucra una investigación difícil. Empezaremos con la siguiente relación general.

VII. Si C y C' son clases del género principal con períodos de m y m' clases, y si M es el menor número divisible por m y m', entonces habrá clases en el mismo género cuyos períodos serán de M términos. Resuelva M en dos factores r y r' primos entre sí, donde uno (r) divide a m, y el otro (r') divide a m' (ver art. 73), y la clase $\frac{m}{r}C + \frac{m'}{r'}C' = C''$ tendrá la propiedad deseada. Pues, supongamos que el período de la clase C'' consiste de g términos, resultará

$$K = grC'' = gmC + \frac{grm'}{r'}C' = K + \frac{grm'}{r'}C' = \frac{grm'}{r'}C'$$

de donde $\frac{grm'}{r'}$ debe ser divisible por m' o gr por r' y así g por r'. De modo semejante se encuentra que g será divisible por r y por lo tanto por $rr' = M$. Pero, puesto que $MC'' = K$, M será divisible por g, y necesariamente $M = g$. Se sigue que el *mayor* número de clases (para un determinante dado) contenido en algún período es

divisible por el número de clases en cualquier otro período (de una clase del mismo género principal). Aquí también puede determinarse un método para encontrar la clase que tiene el mayor período (para un determinante regular este período incluye todo el género principal). Este método es completamente análogo al de los artículos 73 y 74, pero en la práctica puede acortarse el trabajo mediante algunos artificios. El cociente del número n por el número de clases en el período mayor será 1 para determinantes regulares y un entero mayor que 1 para determinantes irregulares, y este cociente es apropiado para expresar los diferentes tipos de irregularidades. Por esta razón se llamará el *exponente de irregularidad*.

VIII. Hasta el momento no hay una regla general mediante la cual puedan distinguirse a priori determinantes regulares de irregulares, en especial porque entre el segundo grupo hay tanto números primos como compuestos; será suficiente entonces agregar algunas observaciones particulares. Cuando se encuentran más de dos clases ambiguas en el género principal, el determinante es irregular y el exponente de irregularidad es par; pero cuando el género tiene sólo uno o dos, el determinante será regular o al menos el exponente de irregularidad será impar. Todos los determinantes negativos de la forma $-(216k + 27)$, excepto -27, son irregulares y el exponente de irregularidad es divisible por 3; lo mismo es válido para los determinantes negativos de la forma $-(1000k + 75)$ y $-(1000k + 675)$, con la excepción de -75, y para una infinidad de otros. Si el exponente de irregularidad es un número primo p, o por lo menos divisible por p, n será divisible por p^2, de donde sigue que si n no admite divisor cuadrado, el determinante es de seguro regular. Es sólo para determinantes positivos *cuadrados* e^2 que puede determinarse a priori si son regulares o irregulares; son regulares si e es 1 ó 2 o un número primo impar o una potencia de un número primo impar; en todos los otros casos son irregulares. Para determinantes negativos, conforme aumentan los determinantes, los irregulares se hacen más frecuentes; e.g., entre los primeros mil encontramos 13 irregulares (omitiendo el signo negativo) 576, 580, 820, 884, 900 cuyo exponente de irregularidad es 2, y 243, 307, 339, 459, 675, 755, 891, 974 cuyo exponente de irregularidad es 3; en el segundo millar hay 13 con exponente de irregularidad 2 y 15 con exponente de irregularidad 3; en el décimo millar hay 31 con exponente de irregularidad 2 y 32 con exponente de irregularidad 3. Todavía no podemos decidir si determinantes con exponente de irregularidad mayor que 3 aparecen debajo de -10000; más allá de este límite puede encontrarse determinantes de cualquier exponente dado. Es muy probable que conforme aumenta el tamaño del determinante, la frecuencia de determinantes negativos irregulares tiende a una razón constante respecto a la frecuencia de los

regulares. La determinación de esta razón sería realmente digna de las habilidades de un geómetra. Para determinantes positivos no cuadrados, los irregulares son mucho más escasos; ciertamente hay un número infinito cuyos exponentes de irregularidad son pares (e.g., 3026 para el cual es 2); y parece haber sin duda algunos cuyos exponentes de irregularidad es impar, aunque debemos confesar que no hemos encontrado ninguno hasta el momento.

IX. Por brevedad, no se puede tratar aquí la disposición más cómoda del sistema de clases contenida en un género principal con determinante irregular; sólo observamos que, puesto que una base no es suficiente, hay que tomar dos o más clases, y a partir de su multiplicación y composición producir todas las demás. Así nacen *índices dobles o múltiples* que tendrán la misma función que los índices simples en el caso de determinantes regulares. Pero trataremos este tema en otra ocasión con más detalle.

X. Finalmente hacemos notar que, puesto que todas las propiedades consideradas en este artículo y el anterior dependen especialmente del número n, el cual juega un papel similar al de $p-1$ en la Sección III, este número merece atención cuidadosa. Es muy deseable por lo tanto determinar la relación general entre este número y el determinante al cual pertenece. No debemos desesperarnos para encontrar la respuesta, puesto que ya hemos logrado establecer (art. 302) la fórmula del valor promedio del producto de n por el número de géneros (que puede determinarse a priori), por lo menos para determinantes negativos.

307.

Las investigaciones de los artículos anteriores sólo toman en cuenta las clases del género principal y así, son suficientes para determinantes positivos cuando hay sólo un género y para determinantes negativos cuando hay sólo un género positivo si no queremos considerar el género negativo. Sólo queda agregar unos cuantos comentarios respecto a los géneros restantes (propiamente primitivos).

I. Cuando G' es un género diferente del género principal G (del mismo determinante) con alguna clase ambigua, habrá tantas en éste como en G. Sean L, M, N, etc. las clases ambiguas en G (entre las cuales estará la clase principal K) y L', M', N', etc., las de G' y designe el primer conjunto por A y el segundo por A'. Puesto que es claro que todas las clases $L+L'$, $M+L'$, $N+L'$, etc., son ambiguas y diferentes entre sí y pertenecen a G', y así también deben estar contenidas en A',

el número de clases en A' no puede ser menor que el número en A, y similarmente, puesto que las clases $L'+L'$, $M'+L'$, $N'+L'$ etc., son diferentes entre sí y ambiguas y pertenecen a G, y por lo tanto están contenidas en A, el número de clases en A no puede ser menor que el número en A'; por esto el número de clases en A y A' son necesariamente iguales.

II. Puesto que el número de todas las clases ambiguas es igual al número de géneros (art. 261, 287.III), es claro que si hay sólo una clase ambigua en G, debe haber una clase ambigua en *cada* género; si hay dos clases ambiguas en G, habrá dos en la mitad de todos los géneros y ninguna en los restantes; finalmente si hay varias clases en G, digamos a de ellas*), la a-ésima parte de todos los géneros contendrá clases ambiguas, el resto no contendrá ninguna.

III. En el caso donde G contiene dos clases ambiguas, sean G, G', G'', etc., los géneros que contienen dos, y H, H', H'', etc., los géneros que no contienen ninguna, y designe el primer conjunto por $\mathfrak{G}$ y el segundo por $\mathfrak{H}$. Puesto que siempre obtenemos una clase ambigua a partir de la composición de dos clases ambiguas (art. 249), no es difícil ver que la composición de dos géneros de $\mathfrak{G}$ siempre da un género de $\mathfrak{G}$. Además, la composición de un género de $\mathfrak{G}$ con un género de $\mathfrak{H}$ da un género de $\mathfrak{H}$; pues, si por ejemplo $G'+H$ no pertenece a $\mathfrak{H}$ sino a $\mathfrak{G}$, $G'+H+G'$ debe estar en $\mathfrak{G}$ *Q. E. A.* , puesto que $G'+G'=G$ y así $G'+H+G'=H$. Finalmente los géneros $G+H$, $G'+H$, $G''+H$, etc. y $H+H$, $H'+H$, $H''+H$, etc. son todos diferentes y así, tomados juntos, deben ser idénticos con $\mathfrak{G}$ y $\mathfrak{H}$; pero por lo que acabamos de mostrar los géneros $G+H$, $G'+H$, $G''+H$, etc. pertenecen todos a $\mathfrak{H}$ y agotan este conjunto; por lo tanto, necesariamente los restantes $H+H$, $H'+H$, $H''+H$, etc. todos pertenecerán a $\mathfrak{G}$: i.e., la composición de dos géneros de $\mathfrak{H}$ siempre da un género de $\mathfrak{G}$.

IV. Si E es una clase del género V, diferente del género principal G, es claro que $2E$, $4E$, $6E$, etc. todos pertenecen a G y $3E$, $5E$, $7E$, etc. a V. Si, por lo tanto, el período de la clase $2E$ contiene m términos, es claro que en la serie E, $2E$, $3E$, etc. la clase $2mE$, y ninguna antes que ella, será idéntica a K; eso es, el período de la clase E contendrá $2m$ términos. Así pues, el número de términos en el período de cualquier clase de un género que no sea el principal será $2n$ o un factor de $2n$, donde n representa el número de clases en todos los géneros.

*) Esto puede suceder sólo para determinantes irregulares y a será siempre una potencia de 2.

V. Sea C una clase dada del género principal G y E una clase del género V que da C cuando se duplica (siempre hay una, art. 286), y sean K, K', K'', etc. clases ambiguas (propiamente primitivas del mismo determinante). Luego $E(= E + K)$, $E + K'$, $E + K''$, etc. serán *todas* las clases que producen C cuando se duplican; este último conjunto se llamará Ω. El número de estas clases será igual al número de clases ambiguas o sea el número de géneros. Habrá tantas clases en Ω que pertenecen al género V como clases ambiguas en G. Por lo tanto, representando este número por a, en cada género habrá a clases de Ω o bien ninguna. Como resultado, cuando $a = 1$, cada género contendrá una clase de Ω; cuando $a = 2$, la mitad de todos los géneros contendrá dos clases de Ω, el resto ninguna. De hecho, la mitad coincidirá totalmente con $\mathfrak{G}$ (según el significado planteado en III) y la segunda mitad con $\mathfrak{H}$ o vice versa. Cuando a es mayor, la a-ésima parte de todos los géneros incluirá clases de Ω (a clases en cada uno).

VI. Supongamos ahora que C es una clase cuyo período contiene n términos. Es obvio que en el caso donde $a = 2$ y n es par, ninguna clase de Ω puede pertenecer a G (puesto que esta clase estaría contenida en el período de la clase C; si fuera $= rC$, eso es $2rC = C$, se tendría $2r \equiv 1 \pmod{n}$ *Q. E. A.*). Por lo tanto, puesto que G pertenece a $\mathfrak{G}$, todas las clases de Ω deben distribuirse entre los géneros $\mathfrak{H}$. De aquí, puesto que (para un determinante regular) hay en total φn clases en G con períodos de n términos, para el caso cuando $a = 2$ habrá en total $2\varphi n$ clases en cada género de $\mathfrak{H}$ con períodos de $2n$ términos que incluirán tanto su propio género como el género principal. Cuando $a = 1$ habrá φn de estas clases en cada género excepto el principal.

VII. Dadas esas observaciones, ahora establecemos el siguiente método para construir el sistema de *todas* las clases propiamente primitivas para cualquier determinante regular dado (puesto que hemos descartado los determinantes irregulares). Escoja arbitrariamente una clase E con período de $2n$ términos. Este período incluirá tanto su propio género que llamamos V como el género principal G; distribuya las clases de estos dos géneros como se presentan en aquel período. El trabajo estará terminado cuando no hay otros géneros salvo estos dos, o cuando no parece ser necesario agregar el resto de ellos (e.g., para un determinante negativo que posee sólo dos géneros positivos). Pero cuando hay cuatro o más géneros, los restantes se tratarán de la siguiente manera. Sea V' uno cualquiera de ellos, y $V + V' = V''$. En V' y V'' habrá dos clases ambiguas (una en cada uno o dos en uno y ninguna en el otro). Seleccione una de éstas, A, de manera arbitraria y es claro que si A se compone con

cada una de las clases en G y V, se producen $2n$ clases distintas que pertenecen a V' y V'' que agotarán completamente estos géneros; por lo tanto estos géneros también se pueden ordenar. Si hay otros géneros además de estos cuatro, sea V''' uno de los restantes y V'''', V''''' y V'''''' los géneros que resultan de la composición de V''' con V, V' y V''. Estos cuatro géneros $V'''\ldots V''''''$ contendrán cuatro clases ambiguas, y si una de ellas, A', se selecciona y se compone con cada una de las clases en G, V, V' y V'', se obtendrán todas las clases en $V'''\ldots V''''''$. Si aún hay más géneros restantes, continúe de la misma manera hasta que todos desaparezcan. Obviamente si el número de géneros construidos es 2^μ, necesitaremos $\mu-1$ clases ambiguas en total, y cada clase de estos géneros se puede generar mediante una multiplicación de la clase E o componiendo una clase que resulta de tal multiplicación con una o más de las clases ambiguas. Siguen dos ejemplos de este procedimiento; no diremos más sobre el uso de tal construcción o de los artificios mediante los cuales se puede facilitar el trabajo.

I. El determinante -161.

Cuatro géneros positivos, cuatro clases cada uno

G	V
1, 4; $R7$; $R23$	3,4; $N7$; $R23$
$(1,\ 0,\ 161) = K$	$(3,\ 1,\ 54) = E$
$(9,\ 1,\ 18) = 2E$	$(6,\ -1,\ 27) = 3E$
$(2,\ 1,\ 81) = 4E$	$(6,\ 1,\ 27) = 5E$
$(9,\ -1,\ 18) = 6E$	$(3,\ -1,\ 54) = 7E$

V'	V''
3, 4; $R7$; $N23$	1,4; $N7$; $N23$
$(7,\ 0,\ 23) = A$	$(10,\ 3,\ 17) = A+E$
$(11,\ -2,\ 15) = A+2E$	$(5,\ 2,\ 33) = A+3E$
$(14,\ 7,\ 15) = A+4E$	$(5,\ -2,\ 33) = A+5E$
$(11,\ 2,\ 15) = A+6E$	$(10,\ -3,\ 17) = A+7E$

II. El determinante −546

Ocho géneros positivos; tres clases en cada uno

G

1 y 3, 8; $R7$; $R7$; $R13$

$(1, \quad 0, 546) = K$
$(22, -2, \quad 25) = 2E$
$(22, \quad 2, \quad 25) = 4E$

V

5 y 7, 8; $N3$; $N7$; $N13$

$(5, \quad 2, 110) = E$
$(21, \quad 0, \quad 26) = 3E$
$(5, \quad -2, 110) = 5E$

V'

1 y 3, 8; $N3$; $R7$; $N13$

$(2, \quad 0, 273) = A$
$(11, -2, \quad 50) = A + 2E$
$(11, \quad 2, \quad 50) = A + 4E$

V''

5 y 7, 8; $R3$; $N7$; $R13$

$(10, \quad 2, \quad 55) = A + E$
$(13, \quad 0, \quad 42) = A + 3E$
$(10, \quad -2, \quad 55) = A + 5E$

V'''

1 y 3, 8; $N3$; $N7$; $R13$

$(3, \quad 0, 182) = A'$
$(17, \quad 7, \quad 35) = A' + 2E$
$(17, -7, \quad 35) = A' + 4E$

V''''

5 y 7, 8; $R3$; $R7$; $N13$

$(15, \quad -3, \quad 37) = A' + E$
$(7, \quad 0, \quad 78) = A' + 3E$
$(15, \quad 3, \quad 37) = A' + 5E$

V'''''

1 y 3, 8; $R3$; $N7$; $N13$

$(6, \quad 0, \quad 91) = A + A'$
$(19, \quad 9, \quad 33) = A + A' + 2E$
$(19, -9, \quad 33) = A + A' + 4E$

V''''''

5 y 7, 8; $N3$; $R7$; $R13$

$(23, \quad 11, \quad 29) = A + A' + E$
$(14, \quad 0, \quad 39) = A + A' + 3E$
$(23, -11, \quad 29) = A + A' + 5E$

Sección Sexta

APLICACIONES VARIAS DE LAS INVESTIGACIONES PRECEDENTES.

308.

A menudo hemos indicado cuán fructífera puede ser la aritmética superior para hechos que pertenecen a otras ramas de la matemática. Por esto vale la pena discutir algunas aplicaciones que merecen más amplio desarrollo, sin embargo, sin intentar agotar un tema que puede fácilmente llenar varios volúmenes. En esta sección trataremos primero de la descomposición de fracciones en otras más simples y de la conversión de fracciones comunes en decimales. Explicaremos luego un método de exclusión que será útil para la solución de ecuaciones indeterminadas de segundo grado. Finalmente, daremos nuevos métodos reducidos para distinguir números primos de números compuestos y para encontrar los factores de estos últimos. En la sección siguiente estableceremos la teoría general de una clase especial de funciones que tiene mucha importancia en todo el análisis y que está estrechamente vinculada con la aritmética superior. En particular agregaremos nuevos resultados a la teoría de secciones de un círculo. Hasta ahora sólo los primeros elementos de esta teoría han sido conocidos.

De la descomposición de fracciones en otras más simples

309.

PROBLEMA. *Descomponer la fracción* $\frac{m}{n}$*, cuyo denominador* n *es el producto de dos números primos relativos* a *y* b *en otras dos cuyos denominadores son* a *y* b*.*

Solución. Sean $\frac{x}{a}$ e $\frac{y}{b}$ las fracciones deseadas; se debe tener $bx + ay = m$; entonces x será una raíz de la congruencia $bx \equiv m \pmod{a}$ que puede ser encontrada por los métodos de la Sección II. Además y será $= \frac{m-bx}{a}$.

Es claro que la congruencia $bx \equiv m$ tiene infinitas raíces, todas conguentes relativas a a; pero hay únicamente una que es positiva y menor que a. También es posible que y sea negativo. Es apenas necesario hacer notar que podemos también encontrar y por la congruencia $ay \equiv m \pmod{b}$ y x por la ecuación $x = \frac{m-ay}{b}$. Por ejemplo, dada la fracción $\frac{58}{77}$, 4 será un valor de la expresión $\frac{58}{11} \pmod{7}$, por tanto $\frac{58}{77}$ se descompondrá en $\frac{4}{7} + \frac{2}{11}$.

310.

Si se propone la fracción $\frac{m}{n}$ con un denominador n, el cual es el producto de cualquier número de factores a, b, c, d, etc. primos entre sí, entonces por el artículo precedente se puede primero resolver en dos fracciones cuyos denominadores serán a y bcd, etc.; luego la segunda de éstas en dos fracciones con denominadores b y cd, etc.; la última de éstas en otras dos y así sucesivamente hasta que toda la fracción dada es reducida a la forma

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \text{ etc.}$$

Evidentemente se pueden tomar los numeradores α, β, γ, δ, etc., positivos y menores que sus denominadores, excepto para el último, el cual ya no es arbitrario cuando los restantes han sido determinados. Este puede ser negativo o mayor que su denominador (si no presuponemos que $m < n$). En tal caso la mayoría de las veces será ventajoso ponerlo en la forma $\frac{\varepsilon}{e} \mp k$ donde ε es positivo y menor que e y k es un entero. Y finalmente a, b, c, etc. pueden ser tomados como números primos o como potencias de números primos.

Ejemplo. La fracción $\frac{391}{924}$ cuyo denominador $= 4 \cdot 3 \cdot 7 \cdot 11$ es resuelta de esta manera en $\frac{1}{4} + \frac{40}{231}$; $\frac{40}{231}$ en $\frac{2}{3} - \frac{38}{77}$; $\frac{-38}{77}$ en $\frac{1}{7} - \frac{7}{11}$ y escribiendo $\frac{4}{11} - 1$ por $-\frac{7}{11}$, tenemos $\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1$.

311.

La fracción $\frac{m}{n}$ puede descomponerse *de una única manera,* en la forma $\frac{\alpha}{a} + \frac{\beta}{b} +$ etc. $\mp k$ tal que α, β, etc., sean positivos y menores que a, b etc.; esto es, suponiendo que

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{ etc.} \mp k = \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + \text{ etc.} \mp k'$$

y si α', β', etc., son también positivos y menores que a, b, etc., tendremos necesariamente $\alpha = \alpha'$, $\beta = \beta'$, $\gamma = \gamma'$, etc., $k = k'$. Porque si multiplicamos por $n = abc$ etc., tenemos $m \equiv \alpha bcd$ etc. $\equiv \alpha' bcd$ etc. (mod. a) y así, puesto que bcd etc. es primo relativo a a, necesariamente $\alpha \equiv \alpha'$ y por lo tanto $\alpha = \alpha'$ y entonces $\beta = \beta'$, etc., de donde inmediatamente $k = k'$. Ahora, puesto que es completamente arbitrario cual denominador es tomado primero, es evidente que *todos* los numeradores pueden ser investigados tal como se hizo con α en el artículo precedente, a saber, β por la congruencia βacd etc. $\equiv m$ (mod. b), γ por γabd etc. $\equiv m$ (mod. c) etc. La suma de todas las fracciones así encontradas será igual a la fracción $\frac{m}{n}$ o la diferencia será el entero k. Esto nos da un medio de verificar el cálculo. Así en el artículo precedente los valores de la expresión $\frac{391}{231}$ (mod. 4), $\frac{391}{308}$ (mod. 3), $\frac{391}{132}$ (mod. 7), $\frac{391}{84}$ (mod. 11), proporcionarán inmediatamente los numeradores 1, 2, 1 y 4 correspondientes a los denominadores 4, 3, 7 y 11 y la suma de estas fracciones excederá a la fracción dada en una unidad.

La conversión de fracciones comunes en decimales.

312.

Definición. Si una fracción común es convertida en un decimal, a la serie de cifras decimales *) (excluyendo la parte entera si la hay), tanto si es finita o infinita, la llamaremos *mantisa* de la fracción. Aquí hemos tomado una expresión, que hasta ahora ha sido usada solamente para logaritmos, y extendido su uso. Así, e.g., la mantisa de la fracción $\frac{1}{8}$ es 125, la mantisa de la fracción $\frac{35}{16}$ es 1875, y la de la fracción $\frac{2}{37}$ es 054054 ... infinitamente repetida.

De la definición, es inmediatamente claro que fracciones del mismo denominador $\frac{l}{n}$ y $\frac{m}{n}$ tendrán la misma o diferente mantisa de acuerdo con que los numeradores

*) Por brevedad restringeremos la discusión siguiente al sistema decimal común, pero puede extenderse fácilmente a cualquiera otro.

l y m sean o no congruentes según n. Una mantisa finita no cambia si se le agrega cualquier número de ceros a la derecha. La mantisa de la fracción $\frac{10m}{n}$ se obtiene desechando de la mantisa de la fracción $\frac{m}{n}$ la primera cifra y en general la mantisa de la fracción $\frac{10^\nu m}{n}$ se encuentra omitiendo las primeras ν cifras de la mantisa de $\frac{m}{n}$. La mantisa de la fracción $\frac{1}{n}$ comienza inmediatamente con una cifra significativa (i.e. diferente de cero) si n no es > 10; pero si $n > 10$ y no igual a una potencia de 10, el número de cifras de las cuales está formada es k, las primeras $k-1$ cifras de la mantisa de $\frac{1}{n}$ serán ceros y la k-ésima será significativa. Por lo tanto, si $\frac{l}{n}$ y $\frac{m}{n}$ tienen mantisas diferentes (i.e. si l y m no son congruentes según n), ellas de hecho no pueden tener las primeras k cifras idénticas, sino que deben diferir al menos en la k-ésima.

313.

PROBLEMA. *Dado el denominador de la fracción $\frac{m}{n}$ y las primeras k cifras de su mantisa, encontrar el numerador m, asumiendo que es menor que n.*

Solución. Consideremos las k cifras como un entero. Multiplique por n y divida el producto por 10^k (u omita las últimas k cifras). Si el cociente es un entero (o todas las cifras omitidas son ceros), será evidentemente el número buscado y la mantisa dada estará completa; de otra forma el numerador que buscamos será el siguiente entero más grande, o el cociente aumentado en una unidad, después de omitir las siguientes cifras decimales. La razón de esta regla se entiende tan fácilmente a partir de lo establecido al final del artículo precedente que no es necesaria una explicación más detallada.

Ejemplo. Si se constata que las dos primeras cifras de la mantisa de una fracción que tienen un denominador 23, es 69, tenemos el producto $23 \cdot 69 = 1587$. Desechando las últimas dos cifras y agregando una unidad, se produce el número 16 para el numerador buscado.

314.

Comenzamos con una consideración de fracciones cuyos denominadores son primos o potencias de primos, y posteriormente reduciremos las demás a este caso. Observamos inmediatamente que la mantisa de la fracción $\frac{a}{p^\mu}$ (suponemos que el numerador a no es divisible por el número primo p) es finita y consiste de μ cifras

cuando $p = 2$ ó $= 5$; en el primer caso esta mantisa, considerada como un entero será $= 5^\mu a$, en el último caso $= 2^\mu a$. Esto es tan obvio que no necesita explicación.

Pero si p es otro número primo, $10^r a$ nunca será divisible por p^μ, no importa cuán grande tomemos a r, y por lo tanto, la mantisa de la fracción $F = \frac{a}{p^\mu}$ debe ser infinita. Supongamos que 10^e es la menor potencia del número 10 que es congruente con la unidad relativo al módulo p^μ (cf. Sección III, donde probamos que e es o igual al número $(p-1)p^{\mu-1}$ o a un divisor de él.) Obviamente $10^e a$ es el primer número en la serie $10a$, $100a$, $1000a$, etc., que es congruente a a relativo al mismo módulo. Ahora ya que, de acuerdo con el artículo 312, obtenemos las mantisas de las fracciones $\frac{10a}{p^\mu}$, $\frac{100a}{p^\mu}$,... $\frac{10^e a}{p^\mu}$ suprimiendo la primera cifra de la fracción F, luego las dos primeras cifras, etc., hasta que se hayan suprimido las e primeras cifras, es evidente que únicamente después de las e primeras cifras, y no antes, las mismas se repetirán. Llamaremos a estas primeras e cifras que forman la mantisa por repetición infinita de ellas mismas el *período* de esta mantisa o de la fracción F. La magnitud del período, i.e. el número e de cifras en él, es completamente independiente del numerador a y es determinado sólo por el denominador. Así, e.g., el período de la fracción $\frac{1}{11}$ es 09 y el período de la fracción $\frac{3}{7}$ es 428571*).

315.

Así cuando se conoce el período de alguna fracción, se puede obtener la mantisa con tantas cifras como queramos. Ahora, si $b \equiv 10^\lambda a \pmod{p^\mu}$, podemos conseguir el período para la fracción $\frac{b}{p^\mu}$ si se escriben las primeras λ cifras del período de la fracción F (suponiendo que $\lambda < e$, lo cual es permisible) después de las restantes $e - \lambda$. Así, junto con el período de la fracción F, tendremos al mismo tiempo los períodos de todas las fracciones cuyos numeradores sean congruentes a los números $10a$, $100a$, $1000a$, etc., relativos al denominador p^μ. Así, e.g., ya que $6 \equiv 3 \cdot 10^2 \pmod{7}$, el período de la fracción $\frac{6}{7}$ se puede deducir inmediatamente del período de la fracción $\frac{3}{7}$, y él es 857142.

Por lo tanto, siempre que 10 es una raíz primitiva (art. 57 y 89) para el módulo p^μ, del período de la fracción $\frac{1}{p^\mu}$ puede deducirse inmediatamente el período de cualquiera otra fracción $\frac{m}{p^\mu}$ (cuyo numerador m no es divisible por p), tomando de la izquierda y escribiendo a la derecha tantas cifras como unidades tenga el índice de

*) Robertson (*Theory of Circulating Fractions, Philos. Trans.* 1769 *p.* 207) indica el comienzo y el final del período por medio de un punto encima de la primera y de la última cifra, algo que no encontramos necesario aquí.

m cuando el número 10 es tomado como base. Así, es claro por qué en este caso el número 10 se tomó siempre como base en la Tabla 1 (ver art. 72).

Cuando 10 no es una raíz primitiva, los únicos períodos de fracciones que pueden ser derivados del período de la fracción $\frac{1}{p^\mu}$ son aquéllos cuyos numeradores son congruentes a alguna potencia de 10 según p^μ. Sea 10^e la más pequeña potencia de 10 que es congruente a la unidad según p^μ; sea $(p-1)p^{\mu-1} = ef$ y tome como base una raíz primitiva r de modo que f sea el índice del número 10 (art. 71). En este sistema, los numeradores de las fracciones cuyos períodos pueden ser derivados del período de la fracción $\frac{1}{p^\mu}$ tendrán como índices f, $2f$, $3f$, $\ldots ef - f$; similarmente, del período de la fracción $\frac{r}{p^\mu}$, podemos deducir períodos para fracciones cuyos numeradores $10r$, $100r$, $1000r$, etc. correspondan a índices $f+1$, $2f+1$, $3f+1$, etc.; del período de la fracción con numerador r^2 (cuyo índice es 2) podemos deducir los períodos de las fracciones cuyos numeradores tienen índices $f+2$, $2f+2$, $3f+2$, etc.; y en general, del período de la fracción con numerador r^i podemos derivar los períodos de fracciones cuyos numeradores tengan índices $f+i$, $2f+i$, $3f+i$, etc. Así, si únicamente se conocen los períodos de las fracciones cuyos numeradores son 1, r, r^2, r^3, $\ldots$, r^{f-1}, se puede obtener todos los otros por transposición sola con la ayuda de la siguiente regla: Sea i el índice del numerador m de una fracción dada $\frac{m}{p^\mu}$ en un sistema donde r es tomado como base (suponemos que i es menor que $(p-1)p^{\mu-1}$); dividiendo por f encontramos $i = \alpha f + \beta$, donde α y β son enteros positivos (ó 0) y $\beta < f$; teniendo esto, podemos encontrar el período de la fracción $\frac{m}{p^\mu}$ a partir del período de la fracción cuyo numerador es r^β (es 1 cuando $\beta = 0$), poniendo las primeras α cifras después de la restantes (cuando $\alpha = 0$ mantenemos el mismo período). Esto explica cómo en la construcción de la Tabla 1 seguimos la regla establecida en el artículo 72.

316.

De acuerdo con estos principios hemos construido una tabla para todos los denominadores de la forma p^μ menores que 1000, que publicaremos íntegramente o incluso con extensiones posteriores si una ocasión se presenta. Por ahora damos como una muestra la Tabla III, que se extiende únicamente hasta 100 y no necesita explicación. Para denominadores que tienen 10 como una raíz primitiva, la tabla da los períodos de las fracciones con numerador 1 (a saber, para 7, 17, 19, 23, 29, 47, 59, 61, 97); para los demás, da los f períodos correspondientes a los numeradores 1, r, r^2, $\ldots$, r^{f-1} que se denominan por los números (0), (1), (2), etc.; para la base r hemos tomado siempre la misma raíz primitiva que en la Tabla I. El período de cualquier

fracción cuyo denominador está contenido en esta tabla puede ser calculado por las reglas dadas en el artículo precedente. Pero, para denominadores muy pequeños podemos ejecutar lo mismo sin la Tabla 1, si por división ordinaria computamos tantas cifras iniciales de la mantisa, de acuerdo con el artículo 313, como sean necesarias para distinguirla de todas las otras del mismo denominador (por la Tabla III no son necesarias más de 2). Ahora examinamos todos los períodos correspondientes al denominador dado, hasta que encontremos estas cifras iniciales, las cuales marcarán el inicio del período. Conviene advertir que estas cifras pueden ser separadas de modo que una (o más) aparezcan al final de un período y las otras al comienzo.

Ejemplo. Búsquese el período de la fracción $\frac{12}{19}$. Para el módulo 19, por Tabla I tenemos $\text{ind.}\, 12 = 2\,\text{ind.}\, 2 + \text{ind.}\, 3 = 39 \equiv 3 \pmod{18}$ (art. 57). Ya que para este caso existe únicamente un período correspondiente al numerador 1, es necesario transponer las primeras tres cifras al final y resulta el período buscado: 631578947368421052. Habría sido igualmente fácil encontrar el comienzo del período por las primeras dos cifras, 63.

Si uno desea el período de la fracción $\frac{45}{53}$, $\text{ind.}\, 45 = 2\,\text{ind.}\, 3 + \text{ind.}\, 5 = 49$, para el módulo 53. El número de períodos aquí es $4 = f$ y $49 = 12f + 1$. De esta forma, del período marcado (1) es necesario transponer las primeras 12 cifras a la posición final y el período buscado es 8490566037735. Las cifras iniciales, 84, están separadas en la tabla.

Observaremos aquí, como prometimos en el artículo 59, que con la ayuda de la Tabla III podemos también encontrar el número que corresponde a un índice dado para un módulo dado (en la tabla el módulo se lista como un denominador). Por esto es claro, de lo que precede, que se puede encontrar el período de una fracción a cuyo numerador (si bien desconocido) corresponde el índice dado. Es suficiente tomar tantas cifras iniciales de este período como cifras haya en el denominador. De esto, por el artículo 313 se encuentra el numerador o el número correspondiente al índice dado.

317.

Por el método precedente, la mantisa de cualquier fracción cuyo denominador es un número primo o una potencia de un número primo dentro de los límites de la tabla, se puede determinar sin cálculo. Pero con la ayuda del resultado del comienzo de esta sección, podemos extender el uso de esta tabla más allá e incluir todas las fracciones cuyos denominadores son productos de primos o potencias de primos

situados dentro de sus límites. Pues, ya que tal fracción puede ser descompuesta en otras cuyos denominadores son estos factores, y éstas pueden ser convertidas en fracciones decimales con cualquier número de cifras, solamente necesitamos combinar todas ellas en una suma. Es apenas necesario hacer notar que la última cifra de la suma puede evidenciar ser poco menos de lo que debiera, pero evidentemente los errores no agregan hacia arriba tantas unidades como fracciones individuales hayan sido agregadas, así, será apropiado computarlas a más cifras que las que se buscan para la fracción dada. Por ejemplo, consideremos la fracción $\frac{6099380351}{1271808720} = F$*), cuyo denominador es el producto de los números 16, 9, 5, 49, 13, 47 y 59. Por las reglas dadas arriba encontramos que $F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59}$; estas fracciones individuales se convierten en decimales como sigue:

$$
\begin{array}{rlll}
1 &= 1 & & \\
\frac{11}{16} &= 0.6875 & & \\
\frac{4}{5} &= 0.8 & & \\
\frac{4}{9} &= 0.4444444444 & 4444444444 & 44 \\
\frac{22}{49} &= 0.4489795918 & 3673469387 & 75 \\
\frac{5}{13} &= 0.3846153846 & 1538461538 & 46 \\
\frac{7}{47} &= 0.1489361702 & 1276595744 & 68 \\
\frac{52}{59} &= 0.8813559322 & 0338983050 & 84 \\
\hline
F &= 4.7958315233 & 1271954166 & 17
\end{array}
$$

El error en esta suma es ciertamente menor que cinco unidades en la vigésima segunda cifra y así las primeras veinte son exactas. Llevando los cálculos a más cifras, encontramos en lugar de las últimas dos cifras, 17, el número 1893936.... Será obvio para todos que este método de convertir fracciones comunes en decimales es especialmente útil cuando buscamos una gran cantidad de cifras decimales; cuando

*) Esta es una de las fracciones que aproxima la raíz cuadrada de 23 y el exceso es menor que siete unidades en la vigésima cifra decimal.

unas pocas bastan, la división ordinaria o los logaritmos pueden ser usados con igual facilidad.

318.

De esta manera, ya que hemos reducido la resolución de tales fracciones con denominador compuesto de varios números primos diferentes al caso en que el denominador es primo o una potencia de un primo, necesitamos agregar solamente unas pocas notas concernientes a sus mantisas. Si el denominador no contiene los factores 2 y 5, la mantisa también consistirá de períodos, porque en este caso la serie 10, 100, 1000, etc. llegará eventualmente a un término que es congruente a la unidad según el denominador. A la vez el exponente de este término, que puede fácilmente determinarse por los métodos del artículo 92, indicará el tamaño del período independientemente del numerador, siempre que sea primo relativo al denominador. Si el denominador es de la forma $2^\alpha 5^\beta N$, donde N designa un número primo relativo a 10, α y β números de los cuales al menos uno no es 0, la mantisa de la fracción llegará a ser periódica después de las primeras α o β cifras (el que sea mayor) y los períodos tendrán la misma longitud que los períodos de fracciones que tienen denominador N. Esto es fácil de ver, ya que la fracción es resoluble en otras dos con denominadores $2^\alpha 5^\beta$ y N, y la primera de ellas cesa enteramente después de las primeras α o β cifras. Podemos fácilmente agregar muchas otras observaciones concernientes a este asunto, especialmente en lo que se refiere a artificios para la construcción de una tabla como la III. Sin embargo omitiremos esta discusión, por motivos de brevedad y porque una gran cantidad de esto ha sido ya publicado por Robertson (loc. cit.) y por Bernoulli (*Nouv. Mém de l'Ac. de Berlin*, 1771, *p.* 273).

Solución de la congruencia $x^2 \equiv A$ por el método de exclusión.

319.

Con respecto a la congruencia $x^2 \equiv A \pmod{m}$, la cual es equivalente a la ecuación indeterminada $x^2 = A + my$, en Sección IV (art. 146) hemos tratado su *posibilidad* de una manera que no parece requerir ningún estudio adicional. Para encontrar la incógnita misma, sin embargo, observamos antes (art. 152) que los métodos indirectos son preferibles a los directos. Si m es un número primo (los otros casos pueden ser reducidos fácilmente a éste), podemos usar la tabla de índices I (combinada con la III de acuerdo con la observación del art. 316) para este propósito,

como lo demostramos más generalmente en el artículo 60, pero el método estará restringido por los límites de la tabla. Por estas razones esperamos que el siguiente método general y conciso placerá a los aficionados de la aritmética.

Primero observamos que es suficiente conocer solamente aquellos valores de x que son positivos y no mayores que $\frac{1}{2}m$, ya que los otros serán congruentes módulo m a uno de éstos, tomado ya sea positiva o negativamente. Para un tal valor de x, el valor de y está necesariamente contenido dentro de los límites $-\frac{A}{m}$ y $\frac{1}{4}m - \frac{A}{m}$. Por ende el método obvio consiste en esto, para cada valor de y contenido dentro de estos límites (denotamos al conjunto de ellos por Ω) computamos el valor de $A + my$ (llamamos a éste, V) y retenemos solamente aquellos valores para los cuales V es un cuadrado. Cuando m es un número pequeño (e.g. abajo de 40), el número de pruebas es tan pequeño que apenas se necesita de un atajo; pero cuando m es grande, la labor puede ser acortada tanto como usted quiera por el siguiente *método de exclusión.*

320.

Sea E un entero arbitrario primo relativo a m y mayor que 2; y sean a, b, c, etc. todos sus no residuos cuadráticos diferentes (i.e. no congruentes según E); y sean α, β, γ, etc. las raíces de las congruencias

$$A + my \equiv a, \qquad A + my \equiv b, \qquad A + my \equiv c, \quad \text{etc.}$$

según el módulo E, con todas estas raíces positivas y menores que E. Si y es un valor congruente a uno de los números α, β, γ, etc., entonces el valor resultante de $V = A + my$ será congruente a uno de los números a, b, c, etc. y así será un no residuo de E y no podrá ser un cuadrado. Así, inmediatamente, pueden excluirse como inservibles todos los valores en Ω que están contenidos en las formas $Et + \alpha$, $Et + \beta$, $Et + \gamma$, etc.; será suficiente examinar a los demás y llamaremos a este conjunto Ω'. En esta operación el número E puede llamarse número *excluyente.*

Tomando otro número excluyente E' apropiado, del mismo modo se encuentran tantos números α', β', γ', etc. como no residuos cuadráticos diferentes haya; y no puede ser congruente a ellos según el módulo E'. Ahora se puede remover de nuevo de Ω' todos los números contenidos en las formas $E't + \alpha'$, $E't + \beta'$, $E't + \gamma'$, etc. De esta manera se puede continuar excluyendo números hasta que aquellos contenidos en Ω sean reducidos hasta el punto que no haya más dificultad en examinar los restantes que en construir nuevas exclusiones.

Ejemplo. Dada la ecuación $x^2 = 22 + 97y$, los límites de los valores de y serán $-\frac{22}{97}$ y $24\frac{1}{4} - \frac{22}{97}$. Así (ya que el valor 0 es obviamente inútil) Ω incluirá los números 1, 2, 3, ... 24. Para $E = 3$ hay únicamente un no residuo, $a = 2$; así $\alpha = 1$. Excluyendo de Ω todos los números de la forma $3t + 1$, Ω' contendrá los 16 números restantes. Similarmente, para $E = 4$ resulta $a = 2$, $b = 3$, y así $\alpha = 0$, $\beta = 1$; y debemos desechar los números de la forma $4t$ y $4t + 1$. Los ocho números restantes son 2, 3, 6, 11, 14, 15, 18 y 23. Igualmente, para $E = 5$ se debe desechar los números de la forma $5t$ y $5t + 3$ y se quedan 2, 6, 11 y 14. Tomando $E = 6$, se deben remover los números de la forma $6t + 1$ y $6t + 4$, pero éstos ya habían sido removidos (ya que son números de la forma $3t + 1$). Tomando $E = 7$, desechamos los números de la forma $7t + 2$, $7t + 3$, $7t + 5$ y se dejan 6, 11 y 14. Si sustituimos y por éstos, dan $V = 604$, 1089 y 1380 respectivamente. Unicamente el segundo valor es un cuadrado, así $x = \mp 33$.

321.

Como la operación con el número excluyente E desecha de los valores de V correspondientes a los valores de y en Ω, todos aquéllos que son no residuos cuadráticos de E, pero no toca los residuos del mismo número, es obvio que el efecto de usar E y $2E$ no difiere si E es impar, ya que en este caso E y $2E$ tienen los mismos residuos y no residuos. Así, si usamos sucesivamente los números 3, 4, 5, etc. como excluyentes, podemos omitir los números $\equiv 2 \pmod 4$, es decir 6, 10, 14, etc., como superfluos. La doble operación, usando E y E' como excluyentes, remueve todos aquellos valores de V que son no residuos de ambos E y E' o de uno de ellos y deja todos los que son residuos de ambos. Ahora, ya que en el caso en que E y E' no tienen un divisor común, los números desechados son todos no residuos y los que permanecen son residuos del producto EE', es evidente que, usando el excluyente EE', se obtendrá en efecto el mismo resultado que usando los dos E y E' y su uso es, por lo tanto, superfluo. Así, es permisible omitir todos aquellos números excluyentes que pueden ser resueltos en dos factores relativamente primos, y es suficiente usar aquéllos que son o primos (no divisores de m) o potencias de primos. Finalmente es claro que, después de usar el número excluyente p^μ que es una potencia del número primo p, los números excluyentes p y p^ν con $\nu < \mu$ son superfluos. Pues, ya que p^μ deja solamente sus residuos de entre los valores de V, ciertamente no habrá no residuos de p o de una potencia menor p^ν. Si p o p^ν fueron usados antes que p^μ, el último evidentemente puede desechar solamente aquellos valores de V que son al

mismo tiempo residuos de p (o p^ν) y no residuos de p^μ; por lo tanto es suficiente tomar para a, b, c, etc., únicamente tales no residuos de p^μ.

322.

El cálculo de los números α, β, γ, etc. correspondientes a cualquier excluyente dado E, puede ser en gran parte abreviado por las siguientes observaciones. Sean $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. raíces de las congruencias $my \equiv a$, $my \equiv b$, $my \equiv c$, etc. (mod. E) y k una raíz de $my \equiv -A$. Es claro que $\alpha \equiv \mathfrak{A} + k$, $\beta \equiv \mathfrak{B} + k$, $\gamma \equiv \mathfrak{C} + k$, etc. Ahora, si fuera necesario encontrar $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. resolviendo estas congruencias, este método de encontrar α, β, γ, etc. no sería más corto que el que hemos mostrado antes; pero esto no es necesario de ningún modo. En efecto, si E es un número primo y m es un residuo cuadrático de E, es claro por el artículo 98 que $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., i.e., los valores de las expresiones $\frac{a}{m}$, $\frac{b}{m}$, $\frac{c}{m}$, etc. (mod. E), son no residuos diferentes de E y así son idénticos con α, β, γ, etc., si no prestamos atención a su orden, el cual de todas formas no importa aquí. Si en la misma suposición m es un no residuo de E, los números $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., son idénticos con todos los residuos cuadráticos, excluyendo el 0. Si E es el cuadrado de un número primo (impar), $= p^2$, y p ya ha sido usado como excluyente, es suficiente, de acuerdo con el artículo precedente, tomar para a, b, c, etc. aquellos no residuos de p^2 que son residuos de p, i.e. los números p, $2p$, $3p$, $\ldots p^2 - p$ (todos los números menores que p^2 que son divisibles por p, excepto 0); entonces para $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., debemos obtener exactamente los mismos números pero en diferente orden. Similarmente, si se pone $E = p^3$ después de aplicar los números excluyentes p y p^2, será suficiente tomar para a, b, c, etc. los productos de cada uno de los no residuos de p por p^2. Como un resultado obtendremos para $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., o los mismos números o los productos de p^2 con cada residuo de p excepto 0, según sea m un residuo o un no residuo de p . En general, tomando para E cualquier potencia de un número primo, digamos p^μ, después de aplicar todas las potencias menores, obtendremos para $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. los productos de $p^{\mu-1}$ por todos los números menores que p excepto 0, cuando μ es par, o por todos los no residuos de p que sean menores que p cuando μ es impar y mRp, o por todos los residuos cuando mNp. Si $E = 4$ y $a = 2$, $b = 3$ tenemos para $\mathfrak{A}$, $\mathfrak{B}$, o 2 y 3 o 2 y 1, según sea $m \equiv 1$ ó $\equiv 3$ (mod. 4). Si después de usar el excluyente 4, ponemos $E = 8$ tendremos $\alpha = 5$ y $\mathfrak{A}$ sería 5, 7, 1, 3 según sea $m \equiv 1, 3, 5, 7$ (mod. 8). En general, si E es una potencia más alta de 2, digamos 2^μ, y todas las potencias menores ya han sido aplicadas, debe ponerse $a = 2^{\mu-1}$, $b = 3 \cdot 2^{\mu-2}$ cuando μ es par. Esto nos da $\mathfrak{A} = 2^{\mu-1}$ y $\mathfrak{B} = 3 \cdot 2^{\mu-1}$ o

$= 2^{\mu-2}$ según sea $m \equiv 1$ o $\equiv 3$. Pero cuando μ es impar, debemos poner $a = 5 \cdot 2^{\mu-3}$ y $\mathfrak{A}$ será igual al producto del número $2^{\mu-3}$ por 5, 7, 1 o 3 según sea $m = 1$, 3, 5 o 7 (mod. 8).

Pero un matemático experto fácilmente encontrará un método para desechar *mecánicamente* los valores de y inservibles que están en Ω después de computar los números α, β, γ, etc. mediante tantas exclusiones como parezcan necesarias. Pero no tenemos espacio para discutir este u otro artificio de economía de trabajo.

Solución de la ecuación indeterminada $mx^2 + ny^2 = A$ por exclusiones.

323.

En la sección V dimos un método general para encontrar todas las representaciones de un A dado por la forma binaria mx^2+ny^2 o sea para encontrar las soluciones de la ecuación indeterminada $mx^2 + ny^2 = A$. El método no deja nada que desear desde el punto de vista de brevedad si ya tenemos todos los valores de la expresión $\sqrt{-mn}$ según el módulo A mismo y según A dividido por sus factores cuadrados. Para el caso, no obstante, en que mn es positivo, daremos una solución que es mucho más corta que la directa cuando aquellos valores no hayan sido computados. Supongamos que los números m, n y A son positivos y primos entre sí, ya que el otro caso puede fácilmente ser reducido a éste. Será suficiente deducir valores positivos de x e y, ya que los otros pueden ser reducidos a éstos por un sencillo cambio de signos.

Claramente x debe ser tal que $\frac{A-mx^2}{n}$, el cual designaremos por V, es positivo, entero, y cuadrado. La primera condición requiere que x no sea mayor que $\sqrt{\frac{A}{m}}$; la segunda se tiene cuando $n = 1$, de otro modo requiere que el valor de la expresión $\frac{A}{m}$ (mod. n) sea un residuo cuadrático de n. Si designamos todos los diferentes valores de la expresión $\sqrt{\frac{A}{m}}$ (mod. n) por $\pm r$, $\pm r'$, etc., x deberá estar contenido en una de las formas $nt + r$, $nt - r$, $nt + r'$, etc. La manera más simple será sustituir x por todos los números de estas formas abajo del límite $\sqrt{\frac{A}{m}}$ (llamaremos a este conjunto Ω) y conservar únicamente aquéllos para los cuales V es un cuadrado. En el siguiente artículo mostraremos cómo reducir el número de estas pruebas tanto como deseemos.

324.

El método de exclusiones por el cual efectuamos esto, tal como en la discusión precedente, consiste en tomar arbitrariamente varios números que nuevamente llamaremos números *excluyentes*, en buscar los valores de x para los cuales el valor

V se convierte en un no residuo de estos números excluyentes y en desechar de Ω estos valores de x. El razonamiento aquí es totalmente análogo al del artículo 321, y así deberemos usar como números excluyentes solamente aquéllos que son primos o potencias de primos, y en el último caso necesitamos desechar solamente aquellos no residuos, entre los valores de V, que son residuos de todas las potencias inferiores del mismo número primo, si es que comenzamos la exclusión con éstas.

Por lo tanto, sea $E = p^\mu$ el número excluyente (incluyendo también el caso donde $\mu = 1$) con p un número primo que no divide m, y supongamos *) que p^ν es la mayor potencia de p que divide a n. Sean a, b, c, etc. no residuos cuadráticos de E (todos ellos cuando $\mu = 1$; los necesarios, i.e. aquéllos que son residuos de potencias inferiores, cuando $\mu > 1$). Compute las raíces α, β, γ, etc. de las congruencias $mz \equiv A - na$, $mz \equiv A - nb$, $mz \equiv A - nc$, etc. (mod. $Ep^\nu = p^{\mu+\nu}$). Es fácil ver que si para algún valor de x resulta $x^2 \equiv \alpha \pmod{Ep^\nu}$, el correspondiente valor de V será $\equiv a \pmod{E}$, esto es, un no residuo de E y similarmente para los restantes números β, γ, etc. Recíprocamente, es igualmente fácil ver que si un valor de x produce $V \equiv a \pmod{E}$, para el mismo valor se hace $x^2 \equiv \alpha \pmod{Ep^\nu}$. Así, todos los valores de x para los cuales x^2 no es congruente a alguno de los números α, β, γ, etc. (mod. Ep^ν) producirán valores de V que no son congruentes a ninguno de los números a, b, c, etc. (mod. E). Ahora se seleccionan de entre los números α, β, γ, etc. todos los residuos cuadráticos g, g', g'', etc. de Ep^ν. Compute los valores de las expresiones $\sqrt{g}$, $\sqrt{g'}$, $\sqrt{g''}$, etc. (mod. Ep^ν) y desígnelos como $\pm h$, $\pm h'$, $\pm h''$, etc. Habiendo hecho esto, todos los números de las formas $Ep^\nu t \pm h$, $Ep^\nu t \pm h'$, $Ep^\nu t \pm h''$, etc. pueden, sin peligro, ser desechados de Ω, y los valores de V contenidos en las formas $Eu + a$, $Eu + b$, $Eu + c$, etc. no pueden corresponder a ningún valor de x en Ω después de esta exclusión. Además es evidente que valores de x en Ω no pueden producir tales valores de V cuando ninguno de los números α, β, γ, etc. es un residuo cuadrático de Ep^ν. En este caso, por consiguiente, el número E no puede ser usado como excluyente. De esta manera se pueden usar tantos números excluyentes como deseemos y consecuentemente disminuir los números en Ω a voluntad.

Veamos ahora si es permisible usar primos que dividen a m o potencias de tales números primos como números excluyentes. Sea B un valor de la expresión $\frac{A}{n} \pmod{m}$; es claro que V será siempre congruente a B según el módulo m, no importa que valor se tome para x. Así, para que la ecuación propuesta sea posible, es necesario que B sea un residuo cuadrático de m. Si p es un divisor primo e impar de

*) Por brevedad consideraremos juntos los dos casos en los cuales n es divisible y no divisible por p; en el segundo caso es necesario hacer $\nu = 0$.

m, por hipótesis, no divide a n o a A y por eso no divide a B. Para cualquier valor de x, V será un residuo de p y así también de cualquier potencia de p; por lo tanto, ni p ni cualquiera de sus potencias pueden ser tomados como excluyentes. Similarmente, cuando m es divisible por 8, para hacer posible la ecuación propuesta, se requiere que $B \equiv 1 \pmod 8$ y así, para cualquier valor de x, V será $\equiv 1 \pmod 8$ y las potencias de 2 no serán idóneas como excluyentes. Sin embargo, cuando m es divisible por 4 pero no por 8, por la misma razón debemos tener $B \equiv 1 \pmod 4$ y el valor de la expresión $\frac{A}{n} \pmod 8$ será o 1 o 5 y lo designaremos por C. Para un valor par de x tendremos $V \equiv C$; para un valor impar $V \equiv C + 4 \pmod 8$. Y así, los valores pares deben ser desechados cuando $C = 5$, y los valores impares cuando $C = 1$. Finalmente, cuando m es divisible por 2 pero no por 4, sea C como antes, un valor de la expresión $\frac{A}{n} \pmod 8$ que será 1, 3, 5 o 7; y sea D un valor de $\frac{\frac{1}{2}m}{n} \pmod 4$ el cual será 1 o 3. Ahora, ya que el valor de V es siempre $\equiv C - 2Dx^2 \pmod 8$ y así para x par, $\equiv C$, para x impar, $\equiv C - 2D$, se sigue que todos los valores impares de x deben ser desechados cuando $C = 1$, todos los valores pares cuando $C = 3$ y $D = 1$ o $C = 7$ y $D = 3$. Todos los valores restantes producirán $V \equiv 1 \pmod 8$; es decir, V es un residuo de alguna potencia de 2. En los casos restantes, a saber, cuando $C = 5$, o $C = 3$ y $D = 3$, o $C = 7$ y $D = 1$, tenemos $V \equiv 3, 5 \text{ o } 7 \pmod 8$, no importa si x es impar o par. Se sigue en estos casos que la ecuación propuesta no tiene solución del todo.

Ahora, de la misma forma en que encontramos x por el método de exclusión, podemos también encontrar y. Así, hay siempre dos maneras de aplicar el método de exclusión para la solución de un problema dado (a menos que $m = n = 1$, cuando los dos coinciden). Deberíamos usualmente escoger aquél para el cual el número de términos Ω es menor, lo que se puede estimar fácilmente por adelantado. Es apenas necesario observar que si, después de un número de exclusiones, *todos* los números en Ω son desechados, esto debe ser considerado como una indicación segura de la imposibilidad de la ecuación propuesta.

325.

Ejemplo. Sea la ecuación dada $3x^2 + 455y^2 = 10857362$. La resolveremos de dos maneras, *primero* investigando los valores de x y luego los valores de y. El límite en x aquí es $\sqrt{3619120\frac{2}{3}}$, el cual cae entre 1902 y 1903; el valor de la expresión $\frac{A}{3} \pmod{455}$ es 354 y los valores de la expresión $\sqrt{354} \pmod{455}$ son ± 82, ± 152,

± 173, ± 212. Así Ω consiste de los siguientes 33 números: 82, 152, 173, 212, 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083, 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902. El número 3 no puede ser usado, en este caso, para exclusión porque divide a m. Para el número excluyente 4, tenemos $a = 2$, $b = 3$ así $\alpha = 0$, $\beta = 3$, $g = 0$ y los valores de la expresión $\sqrt{g}$ (mod. 4) son 0 y 2; así, todos los números de la forma $4t$ y $4t + 2$, i.e. todos los números pares, deben ser desechados de Ω; denotaremos los 16 restantes por Ω'. Para $E = 5$, el cual también divide a n, las raíces de las congruencias $mz \equiv A - 2n$ y $mz \equiv A - 3n$ (mod. 25) son 9 y 24, ambos residuos de 25. Los valores de las expresiones $\sqrt{9}$ y $\sqrt{24}$ (mod. 25) son ± 3, ± 7. Cuando desechamos de Ω' todos los números de las formas $25t \pm 3$, $25t \pm 7$, allí permanecen estos diez (Ω''): 173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577. Para $E = 7$ las raíces de las congruencias $mz \equiv A - 3n$, $mz \equiv A - 5n$, $mz \equiv A - 6n$ (mod. 49) son 32, 39, 18, todas ellas residuos de 49, y los valores de las expresiones $\sqrt{32}$, $\sqrt{39}$, $\sqrt{18}$ (mod. 49) son ± 9, ± 23, ± 19. Cuando desechamos de Ω'' los números de las formas $49t \pm 9$, $49t \pm 19$ y $49t \pm 23$, estos cinco (Ω''') permanecen: 537, 737, 1083, 1213, 1517. Para $E = 8$ tenemos $a = 5$, así $\alpha = 5$, un no residuo de 8; por lo tanto el excluyente 8 no puede ser usado. El número 9 debe ser desechado por la misma razón que 3. Para $E = 11$ los números a, b, etc. se convierten en 2, 6, 7, 8, 10; $\nu = 0$; así los números α, β, etc. $= 8, 10, 5, 0, 1$. Tres de ellos, 0, 1, 5 son residuos de 11 y por esta razón desechamos de Ω''' los números de las formas $11t$, $11t \pm 1$, $11t \pm 4$. Permanecen los números 537, 1083, 1213. Usando éstos obtenemos para V los valores 21961, 16129, 14161 respectivamente. Solamente el segundo y el tercero son cuadrados. Así la ecuación dada admite solamente dos soluciones con valores positivos de x e y: $x = 1083$, $y = 127$ y $x = 1213$, $y = 119$.

Segundo. Si preferimos encontrar la otra incógnita de esta misma ecuación por exclusiones, intercambiamos x e y y la escribimos como $455x^2 + 3y^2 = 10857362$, así que podemos retener la notación de los artículos 323 y 324. El límite para los valores de x cae entre 154 y 155; el valor de la expresión $\frac{A}{m}$ (mod. n) es 1; los valores de $\sqrt{1}$ (mod. 3) son $+1$ y -1. Por lo tanto Ω contiene todos los números de las formas $3t+1$ y $3t - 1$, es decir, todos los números hasta 154 inclusive que no son divisibles por 3, de los cuales hay 103. Aplicando las reglas dadas arriba para excluir 3, 4, 9, 11, 17, 19 y 23, debemos desechar los números de las formas $9t \pm 4$; $4t$, $4t \pm 2$, o sea todos los pares; $27t \pm 1$, $27t \pm 10$; $11t$, $11t \pm 1$, $11t \pm 3$; $17t \pm 3$, $17t \pm 4$, 17 ± 5, $17t \pm 7$; $19t \pm 2$, $19t \pm 3$, $19t \pm 8$, $19t \pm 9$; $23t$, $23t \pm 1$, $23t \pm 5$, $23t \pm 7$, $23t \pm 9$, $23t \pm 10$. Después de que todos éstos han sido suprimidos, hemos dejado los números 119 y 127, que dan

a V un valor cuadrado y producen las mismas soluciones que obtuvimos arriba.

326.

Los métodos precedentes son ya tan concisos que dejan muy poco que desear. No obstante hay muchos artificios, para acortar la operación, de los cuales podemos tocar aquí solamente unos pocos. Por lo tanto restringiremos nuestra discusión al caso en el que el número excluyente es un primo impar que no divide a A, o una potencia de un tal primo. Los casos restantes pueden ser tratados de modo análogo o reducidos a éste. Suponiendo *primero* que el número excluyente $E = p$ es un primo que no divide ni a m ni a n y los valores de las expresiones $\frac{A}{m}$, $-\frac{na}{m}$, $-\frac{nb}{m}$, $-\frac{nc}{m}$, etc. (mod. p) son k, $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. respectivamente, se obtienen los números α, β, γ, etc. de las congruencias $\alpha \equiv k + \mathfrak{A}$, $\beta \equiv k + \mathfrak{B}$, $\gamma \equiv k + \mathfrak{C}$, etc. (mod. p). Los números $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc. pueden ser determinados, sin calcular las congruencias, por un artificio muy parecido al que usamos en el artículo 322, y serán idénticos con todos los no residuos o con todos los residuos de p (excepto 0), de acuerdo con el valor de la expresión $-\frac{m}{n}$ (mod. p), o (lo que es la misma cosa) según sea el número $-mn$ un residuo o un no residuo de p. Así, en el ejemplo II del artículo precedente, para $E = 17$ tenemos $k = 7$; $-mn = -1365 \equiv 12$ es un no residuo de 17; así, los números $\mathfrak{A}$, $\mathfrak{B}$, etc. serán 1, 2, 4, 8, 9, 13, 15, 16 y los números α, β, etc. serán 8, 9, 11, 15, 16, 3, 5, 6. Los residuos entre ellos son 8, 9, 15 y 16, así $\pm h$, h', etc. se convierten en ± 5, 3, 7, 4. Quienes hayan resuelto a menudo problemas de este tipo encontrarán esto extremadamente útil si calculan para varios números primos p los valores de h, h', etc. correspondientes a valores individuales de k (1, 2, 3, $\ldots p-1$) bajo la doble suposición (a saber, donde $-mn$ es un residuo y donde es un no residuo de p). Observamos que hay siempre $\frac{1}{2}(p-1)$ números h, $-h$, h', etc. cuando los números k y $-mn$ son ambos residuos o ambos no residuos de p; $\frac{1}{2}(p-3)$ números cuando el primero es un residuo y el último un no residuo; $\frac{1}{2}(p+1)$ números cuando el primero es un no residuo y el último un residuo; pero debemos omitir la demostración de este teorema para no ser demasiado prolijos.

Segundo, podemos explicar un tanto expeditamente los casos cuando E es un número primo que divide a n, o la potencia de un número primo (impar) que divide o no divide a n. Trataremos todos estos casos juntos y, reteniendo la notación del artículo 324, pondremos $n = n'p^\nu$ tal que n' no es divisible por p. Los números a, b, c, etc. serán los productos del número $p^{\mu-1}$ por todos los números menores que p (excepto 0) o por todos los no residuos de p menores que p, según μ sea par o

impar. Expresamos esto indefinidamente por $up^{\mu-1}$. Sea k el valor de la expresión $\frac{A}{m} \pmod{p^{\mu+\nu}}$, el cual no será divisible por p porque A no lo es. Todos los α, β, γ, etc. serán congruentes a k módulo p, y así p^μ no excluirá nada de Ω si kNp. Si realmente kRp y así también $kRp^{\mu+\nu}$, sea r un valor de la expresión $\sqrt{k} \pmod{p^{\mu+\nu}}$ que no es divisible por p, y sea e el valor de $-\frac{n'}{2mr} \pmod{p}$. Entonces tendremos $\alpha \equiv r^2 + 2erap^\nu \pmod{p^{\mu+\nu}}$ y claramente α es un residuo de $p^{\mu+\nu}$ y los valores de la expresión $\sqrt{\alpha} \pmod{p^{\mu+\nu}}$ se convierten en $\pm(r + eap^\nu)$, así, todos los h, h', h'', etc. son expresados por $r + uep^{\mu+\nu-1}$. Finalmente concluimos que los números h, h', h'', etc. provienen de la adición del número r con los productos del número $p^{\mu+\nu-1}$ por todos los números menores que p (excepto 0) cuando μ es par; o por todos los no residuos de p menores que este límite cuando μ es impar y eRp o, lo que viene a ser la misma cosa, cuando $-2mrn'Rp$; o por todos los residuos (excepto 0) cuando μ es impar y $-2mrn'Np$.

Pero exactamente como encontramos los números h, h', etc. para cada uno de los números excluyentes, será posible ejecutar la misma exclusión por operaciones mecánicas que el experto puede desarrollar fácilmente si esto le parece útil.

Finalmente debemos observar que cualquier ecuación $ax^2 + 2bxy + cy^2 = M$ en la que $b^2 - ac$ es negativo, digamos $-D$, puede ser fácilmente reducida a la forma que consideramos en el artículo precedente. Porque si hacemos m el máximo común divisor de los números a y b, y ponemos

$$a = ma', \qquad b = mb', \qquad \frac{D}{m} = a'c - mb'^2 = n, \qquad a'x + b'y = x'$$

la ecuación será equivalente a $mx'^2 + ny^2 = a'M$. Esto puede ser resuelto por las reglas que dimos antes. Solamente van a ser retenidas aquellas soluciones en las cuales $x' - b'y$ es divisible por a', i.e. las que dan valores enteros de x.

Otro método de resolver la congruencia $x^2 \equiv A$ para el caso en que A es negativo.

327.

La solución directa de la ecuación $ax^2 + 2bxy + cy^2 = M$ contenida en la sección V asume que conocemos los valores de la expresión $\sqrt{b^2 - ac} \pmod{M}$. Recíprocamente, en el caso donde $b^2 - ac$ es negativo, la solución indirecta anterior da un método muy rápido de encontrar tales valores y es preferible al método del artículo 322 y siguientes, especialmente para un valor muy grande de M. Pero supondremos que M es un número primo o, al menos, si es compuesto, que sus factores son empero

desconocidos. Pues si fuera claro que el número primo p divide a M y si $M = p^\mu M'$ de tal forma que M' no involucre el factor p, sería más conveniente explorar los valores de la expresión $\sqrt{b^2 - ac}$ para los módulos p^μ y M' separadamente (obteniendo el primero de los valores según el módulo p, art. 101) y luego deducir los valores según el módulo M de su combinación (art. 105).

Entonces, es necesario buscar todos los valores de la expresión $\sqrt{-D}$ (mod. M) donde D y M son positivos, y M está contenido en una forma de los divisores de $x^2 + D$ (art. 147 y siguientes). De otro modo sería a priori evidente que no hay números que satisfagan la expresión dada. Los valores buscados serán siempre opuestos dos a dos. Sean ellos $\pm r$, $\pm r'$, $\pm r''$, etc., y $D + r^2 = Mh$, $D + r'^2 = Mh'$, $D + r''^2 = Mh''$, etc.; posteriormente designe las clases a las cuales corresponden las formas (M, r, h), $(M, -r, h)$, (M, r', h'), $(M, -r', h')$, (M, r'', h''), $(M, -r'', h'')$, etc. respectivamente por $\mathfrak{C}$, $-\mathfrak{C}$, $\mathfrak{C}'$, $-\mathfrak{C}'$, $\mathfrak{C}''$, $-\mathfrak{C}''$, etc. y al conjunto de ellas por $\mathfrak{G}$. Hablando en general, estas clases son las que serán consideradas como incógnitas. Sin embargo es claro *primero,* que todas ellas son positivas y propiamente primitivas, *segundo,* que ellas corresponden al mismo género cuyo *carácter* es fácilmente reconocible a partir de la naturaleza del número M, i.e. de sus relaciones con cada uno de los divisores primos de D (y con 4 u 8 cuando sea necesario) (cf. art. 230). Ya que suponemos que M está contenido en una forma de los divisores de $x^2 + D$, sabemos a priori que de seguro hay un género positivo propiamente primitivo de determinante $-D$ para este carácter aún cuando no haya valores de la expresión $\sqrt{-D}$ (mod. M). Ya que, por lo tanto, este género es conocido, se puede encontrar todas las clases contenidas en él. Desígnense como C, C', C'', etc. y el conjunto de ellas por G. Es claro entonces que las clases individuales $\mathfrak{C}$, $-\mathfrak{C}$, etc. deben ser idénticas con clases en G; también puede suceder que varias clases en $\mathfrak{G}$ sean idénticas unas a otras y con la misma clase en G; y cuando G contiene solamente una clase, de seguro todas las clases en $\mathfrak{G}$ coincidirán con ella. Por lo tanto si de las clases C, C', C'', etc. seleccionamos las (más simples) formas f, f', f'', etc. (una de cada una), de entre éstas aparecerá una forma de cada clase en $\mathfrak{G}$. Ahora, si $ax^2 + 2bxy + cy^2$ es una de las formas contenidas en $\mathfrak{C}$, existirán dos representaciones del número M correspondiendo al valor r por esta forma, y si una es $x = m$, $y = n$, la otra será $x = -m$, $y = -n$. La única excepción ocurre cuando $D = 1$, en cuyo caso existirán cuatro representaciones (ver art. 180).

Se sigue de esto que si se encuentran todas las representaciones del número M por las formas individuales f, f', f'', etc. (usando el método indirecto de los artículos precedentes) y deducimos de éstos los valores de la expresión $\sqrt{-D}$ (mod. M) a la

cual cada una pertenece (art. 154 y siguientes), obtendremos *todos* los valores de esta expresión, y realmente cada uno de ellos dos veces o, si $D = 1$, cuatro veces. *Q. E. F.* Si encontramos alguna forma entre las f, f', etc. por la cual M no puede ser representada, esto es una indicación de que ella no pertenece a una clase en $\mathfrak{G}$ y así puede ser olvidada. Pero si M no puede ser representada por ninguna de esta formas, $-D$ es necesariamente un no residuo cuadrático de M. Tocante a estas operaciones se tienen las siguientes observaciones.

I. Las representaciones del número M por las formas f, f', etc. que usamos aquí son aquéllas en las cuales los valores de las incógnitas son primos relativos; si aparecen otras en las que estos valores tienen un divisor común μ (esto puede suceder solamente cuando μ^2 divide a M, y sucede con seguridad cuando $-DR\frac{M}{\mu^2}$), ellas serán completamente desatendidas para nuestros presentes propósitos, aún cuando pueden ser útiles en otros contextos.

II. Siendo otras cosas iguales, es obvio que la labor implicada será más fácil cuando el número de clases f, f', f'', etc. sea menor. Por consiguiente, esto es lo más corto posible cuando D es uno de los 65 números tratados en el artículo 303, porque tienen solamente una clase en cada género.

III. Dado que existen siempre dos representaciones $x = m$, $y = n$ y $x = -m$, $y = -n$ correspondiendo al mismo valor, es obviamente suficiente considerar únicamente aquellas representaciones en las cuales y es positivo. *Tales* representaciones diferentes corresponderán siempre a diferentes valores de la expresión $\sqrt{-D}$ (mod. M), y el número de todos los valores diferentes será igual al número de tales representaciones (siempre exceptuando el caso cuando $D = 1$ donde el primer número será la mitad del segundo).

IV. Puesto que, tan pronto como conocemos uno de los dos valores opuestos $+r$, $-r$, conocemos inmediatamente el otro, las operaciones pueden ser abreviadas un tanto. Si el valor se obtiene de la representación del número M por una forma contenida en la clase C, i.e. si $\mathfrak{C} = C$, el valor opuesto $-r$ evidentemente proviene de la representación por una forma contenida en la clase que es opuesta a C, y esta clase siempre será diferente de C a menos que C sea ambigua. Se sigue que cuando no todas las clases en G son ambiguas, solamente la mitad de las restantes necesitan ser consideradas. Se puede omitir una de cada par de opuestos e inmediatamente

escribir ambos valores después de haber calculado solamente uno. Cuando C es ambigua, ambos valores r y $-r$ emergerán al mismo tiempo; es decir, si tomamos la forma ambigua $ax^2 + 2bxy + cy^2$ de C y el valor r es producido por la representación $x = m$, $y = n$, el valor $-r$ resultará de la representación $x = -m - \frac{2bn}{a}$, $y = n$.

V. Para el caso donde $D = 1$, existe únicamente una clase, de la cual podemos seleccionar la forma $x^2 + y^2$. Si el valor r resulta de la representación $x = m$, $y = n$, resultará también de $x = -m$, $y = -n$; $x = n$, $y = -m$; $x = -n$, $y = m$ y el opuesto, $-r$, resultará de $x = m$, $y = -n$; $x = -m$, $y = n$; $x = n$, $y = m$; $x = -n$, $y = -m$. Así de estas ocho representaciones que constituyen únicamente una descomposición, una es suficiente en tanto que asociemos el valor opuesto con el que resulta de nuestra investigación.

VI. El valor de la expresión $\sqrt{-D}$ (mod. M) al cual corresponde la representación $M = am^2 + 2bmn + cn^2$ es, por artículo 155, $\mu(mb + nc) - \nu(ma + nb)$ o cualquier número congruente a él según M, donde los números μ y ν satisfacen $\mu m + \nu n = 1$. Designando este valor por v, tendremos

$$mv \equiv \mu m(mb+nc) - \nu(M - mnb - n^2c) \equiv (\mu m + \nu n)(mb+nc) \equiv mb+nc \pmod{M}$$

Así, es claro que si v es un valor de la expresión $\frac{mb+nc}{m}$ (mod. M); similarmente se encuentra que es un valor de la expresión $-\frac{ma+nb}{n}$ (mod. M). Estas fórmulas son muy a menudo preferidas a aquélla de la cual fueron deducidas.

328.

Ejemplos. I. Búsquense todos los valores de la expresión $\sqrt{-1365}$ (mod. $5428681 = M$); el número M es $\equiv 1, 1, 1, 6, 11$ (mod. 4, 3, 5, 7, 13) y así está contenido en una forma de los divisores de $x^2 + 1$, $x^2 + 3$, $x^2 - 5$ y en una forma de los no divisores de $x^2 + 7$, $x^2 - 13$ y por lo tanto en una forma de los divisores de $x^2 + 1365$; el carácter del género en el cual se encontrarán las clases $\mathfrak{G}$, es 1, 4; $R3$; $R5$; $N7$; $N13$. Existe solamente una clase contenida en este género y de ésta seleccionaremos la forma $6x^2+6xy+229y^2$. Para encontrar todas las representaciones del número M por esta forma, ponemos $2x + y = x'$ y tenemos $3x'^2 + 455y^2 = 2M$. Esta ecuación admite cuatro soluciones en las que y es positivo, a saber $y = 127$,

$x' = \pm 1083$, $y = 119$, $x' = \pm 1213$. De éstas obtenemos cuatro soluciones de la ecuación $6x^2 + 6xy + 229y^2 = M$ en las que y es positivo,

x	478	-605	547	-666
y	127	127	119	119

La primera solución da para v el valor de la expresión $\frac{30517}{478}$ o $\frac{-3249}{127}$ (mod. M) y encontramos que es 2350978; la segunda produce el valor opuesto -2350978; la tercera, el valor 2600262; y la cuarta, su opuesto -2600262.

II. Si queremos los valores de la expresión $\sqrt{-286}$ (mod. $4272943 = M$), el carácter del género en el que están contenidas las clases $\mathfrak{G}$, será 1 y 7, 8; $R11$; $R13$. Este será por lo tanto el género principal en el cual están contenidas tres clases, representadas por las formas $(1, 0, 286)$, $(14, 6, 23)$ y $(14, -6, 23)$. Se puede omitir la tercera de éstas, ya que es opuesta a la segunda. Por la forma $x^2 + 286y^2$ encontramos dos representaciones del número M en las que y es positivo, a saber, $y = 103$, $x = \pm 1113$. De ellas deducimos estos valores para la expresión dada: 1493445 y -1493445. Encontramos que M no es representable por la forma $(14, 6, 23)$ y concluimos que ésos son los únicos valores.

III. Dada la expresión $\sqrt{-70}$ (mod. 997331), las clases $\mathfrak{G}$ deben estar contenidas en el género cuyo carácter es 3 y 5, 8; $R5$; $N7$. Hay únicamente una clase y su forma representante es $(5, 0, 14)$. Después de un cálculo se encuentra que el número 997331 no es representable por la forma $(5, 0, 14)$ y así -70 será necesariamente un no residuo cuadrático de ese número.

Dos métodos para distinguir números compuestos de números primos y para determinar sus factores.

329.

El problema de distinguir números primos de números compuestos y de resolver estos últimos en sus factores primos es conocido como uno de los más importantes y útiles en aritmética. Ha ocupado la industria y la sabiduría de geómetras antiguos y modernos a tal grado que sería superfluo discutir el problema detenidamente. No obstante debemos admitir que todos los métodos que han sido propuestos hasta ahora son o restringidos a casos muy especiales o tan laboriosos y prolijos que aún para números que no exceden los límites de tablas construidas por hombres estimables, i.e., para números que no requieren métodos ingeniosos, ponen a prueba la paciencia hasta de los calculistas experimentados. Y estos métodos a duras

penas pueden ser usados para números grandes. Aún cuando las tablas, que están disponibles para quien quiera y las cuales esperamos continuarán siendo extendidas, son realmente suficientes para la mayoría de los casos ordinarios, frecuentemente sucede que el calculista entrenado obtendrá la suficiente ganancia de la reducción de números grandes a sus factores de modo que esto lo compensará por el tiempo consumido. Luego, la dignidad de la ciencia misma parece requerir que todos los medios posibles para la solución de un problema tan elegante y tan célebre sean explorados. Por esta razón, no dudamos que los dos métodos siguientes, cuya eficacia y brevedad podemos confirmar a partir de una larga experiencia, resultarán gratificantes a los aficionados a la aritmética. Está en la naturaleza del problema que *cualquier* método se hará más prolijo a medida que los números se hacen mayores. No obstante, en los siguientes métodos, las dificultades crecen algo lentamente, y números con siete, ocho o aún más dígitos han sido manipulados con éxito y rapidez más allá de la esperada, especialmente por el segundo método. Las técnicas que fueron previamente conocidas requerirían un trabajo intolerable aún para el calculista más infatigable.

Antes de considerar los siguientes métodos, es siempre muy útil tratar de dividir el número dado por algunos de los primos más pequeños, digamos por 2, 3, 5, 7, etc. hasta 19 o un poco más allá, a fin de eludir el uso de métodos sutiles y artificiales cuando la sola división puede ser más sencilla *); y también, porque cuando la división no es exitosa, la aplicación del segundo método utiliza con gran beneficio los *residuos* derivados de estas divisiones. Así, e.g., si el número 314159265 se va a resolver en sus factores, la división por 3 es exitosa dos veces, y después, las divisiones por 5 y por 7. Así tenemos $314159265 = 9 \cdot 5 \cdot 7 \cdot 997331$ y es suficiente examinar por medios más sutiles el número 997331, el cual no es divisible por 11,13,17 ni 19. Similarmente, dado el número 43429448, podemos remover el factor 8 y aplicar los métodos más sutiles al cociente 5428681.

330.

El fundamento del PRIMER METODO es el teorema que establece que *cualquier número positivo o negativo que es un residuo cuadrático de otro número M, es también un residuo de cualquier divisor de M.* Cualquiera sabe que si M no es divisible por ningún número primo abajo de $\sqrt{M}$, M es de seguro primo; pero si todos

*) Aún más, puesto que, generalmente hablando, entre cualesquiera seis números dados difícilmente habrá *uno* que no sea divisible por uno de los números 2, 3, 5, ... 19.

los números primos abajo de este límite que dividen a M son p, q, etc., el número M está compuesto por éstos *solamente* (o por sus potencias), o existe únicamente *un* factor primo mayor que $\sqrt{M}$. Este se encuentra dividiendo M por p, q, etc. tantas veces como se pueda. Por lo tanto, si designamos el conjunto de todos los números primos abajo de $\sqrt{M}$ (excluyendo a aquéllos que ya sabemos que no dividen al número) por Ω, evidentemente será suficiente encontrar todos los divisores de M contenidos en Ω. Ahora, si de alguna manera se constata que un número r (no cuadrado) es un residuo cuadrático de M, de seguro ningún número primo del cual r es un no residuo puede ser un divisor de M; por consiguiente se pueden remover de Ω todos los números primos de este tipo (ellos usualmente conformarán alrededor de la mitad de los números de Ω). Y si llega a ser claro que otro número r' no cuadrado es un residuo de M, podemos excluir de los restantes números primos en Ω aquellos para los cuales r' es un no residuo. De nuevo reducimos estos números en casi la mitad, siempre y cuando los residuos r y r' sean independientes (i.e. a menos que uno de ellos sea necesariamente un residuo de todos los números de los cuales el otro es un residuo; esto sucede cuando rr' es un cuadrado). Si todavía conocemos otros residuos r'', r''', etc. de M, cada uno de ellos independiente de los restantes*), podemos instituir exclusiones similares con cada uno de ellos. Así, la cantidad de números en Ω disminuirá rápidamente hasta que todos ellos sean removidos, en cuyo caso M será ciertamente un número primo, o quedarán tan pocos (obviamente todos los divisores primos de M aparecerán entre ellos, si existe alguno) que la división por ellos puede ser probada sin demasiada dificultad. Para un número que no excede un millón aproximadamente, usualmente seis o siete exclusiones serán suficientes; para un número con ocho o nueve dígitos, de seguro serán suficientes nueve o diez exclusiones. Resta ahora hacer dos cosas, *primero* encontrar residuos apropiados de M y un número suficiente de ellos, *entonces* efectuar la exclusión de la manera más conveniente. Pero invertiremos el orden de las cuestiones porque lo segundo nos mostrará cuales residuos son los más apropiados para este propósito.

331.

En la sección IV hemos mostrado detenidamente como distinguir números

*) Si el producto de cualquier cantidad de números r, r', r'', etc. es un cuadrado, cada uno de ellos, e.g. r, será un residuo de cualquier número primo (que no divida a ninguno de ellos) que sea un residuo de los otros, r', r'', etc. Así, para que los residuos sean independientes, ningún producto de pares o triples, etc. de ellos puede ser cuadrado.

primos para los cuales un r dado es un residuo (podemos suponer que no es divisible por un cuadrado) de aquéllos para los cuales es un no residuo; es decir, como distinguir los divisores de la expresión $x^2 - r$ de los no divisores. Todos los divisores están contenidos bajo fórmulas como $rz + a$, $rz + b$, etc. o como $4rz + a$ y $4rz + b$, etc. y los otros bajo fórmulas semejantes. Siempre que r es un número muy pequeño, con la ayuda de estas fórmulas podemos llevar a cabo las exclusiones satisfactoriamente; e.g. cuando $r = -1$ todos los números de la forma $4z + 3$ serán excluidos; cuando $r = 2$ se excluyen todos los números de las formas $8z + 3$ y $8z + 5$, etc. Pero puesto que no siempre es posible encontrar residuos como éstos para un número M dado, y la aplicación de las fórmulas no es muy conveniente cuando el valor de r es grande, se ganará mucho y el trabajo de exclusión se reducirá sobremanera si tenemos una *tabla* para una cantidad suficientemente grande de números (r) tanto positivos como negativos que no sean divisibles por cuadrados. La tabla deberá distinguir números primos que tengan a cada uno (r) como residuo de aquéllos para los cuales es un no residuo. Tal tabla puede ser arreglada del mismo modo que el ejemplo al final de este libro que ya hemos descrito arriba; pero a fin de que ella sea útil para nuestros propósitos presentes, los números primos (módulos) en el margen deben ser continuados mucho más lejos, a 1000 o 10000. Sería aún más conveniente si los números compuestos y negativos también fueran listados hasta el tope, aunque esto no es absolutamente necesario, como es claro de la sección IV. La máxima utilidad resultaría si las columnas verticales individuales fueran removibles y pudieran ser rearmadas sobre placas o varillas (como las de Napier). Entonces aquéllos que son necesarios en cada caso, i.e. los que corresponden a r, r', r'', etc., los residuos de los números dados, pueden ser examinados separadamente. Si éstos son colocados *correctamente* junto a la primera columna de la tabla (que contiene al módulo), i.e. de manera que la posición en cada una de las varillas que corresponden al mismo número en la primera columna es puesta en la línea horizontal correspondiente, aquellos números primos que permanecen después de las exclusiones de Ω correspondientes a los residuos r, r', r'', etc. pueden ser inmediatamente reconocidos por inspección. Ellos son los números en la primera columna que tienen pequeñas ranuras en *todas* las varillas adyacentes. Un primo para el que *alguna* varilla tiene un espacio vacío debe ser desechado. Un ejemplo ilustrará esto suficientemente bien. Si de algún modo sabemos que los números -6, $+13$, -14, $+17$, $+37$, -53 son residuos de 997331, entonces acoplaríamos juntas la primera columna (la cual en este caso sería continuada hasta el número 997, i.e. hasta el mayor número primo menor que $\sqrt{997331}$) y las columnas que tengan como tope los números -6, $+13$, etc. He aquí

una sección de este esquema:

	−6	+13	−14	+17	+37	−53
3	—	—	—		—	—
5	—		—			
7	—		—		—	
11	—				—	
13		—	—	—		—
17		—		—		—
19			—	—		—
23		—	—			—
			etc.			
113		—	—			—
127	—	—	—	—	—	—
131	—	—	—			
			etc.			

Así, por inspección, de aquellos primos *contenidos en esta parte del esquema*, se sabe que después de todas las exclusiones con los residuos −6, 13, etc. únicamente permanece en Ω el número 127. El esquema total extendido hasta el número 997 mostraría que no hay otro número en Ω. Cuando probamos esto, encontramos que 127 efectivamente divide a 997331. De esta manera encontramos que este número puede ser resuelto en los factores primos $127 \cdot 7853$*).

De este ejemplo es suficientemente claro que aquellos residuos especialmente útiles son los no demasiado grandes, o que al menos pueden ser descompuestos en factores primos que no son demasiado grandes. El uso directo de la tabla auxiliar no se extiende más allá de los números a la cabeza de las columnas, y el uso indirecto sólo incluye aquellos números que pueden ser resueltos en factores contenidos en la tabla.

*) El autor ha construido para su propio uso una gran parte de la tabla descrita aquí y la habría publicado gustosamente si el pequeño número de aquéllos para quienes sería útil bastase para justificar tal empresa. Si hay algún devoto de la aritmética que comprende los principios involucrados y desea construir una tabla como ésta por sí mismo, el autor encontrará gran placer en comunicarle mediante carta todos los procedimientos y artificios que usó.

332.

Daremos tres métodos para encontrar residuos de un número M dado, pero antes de explicar esto queremos hacer dos observaciones que nos ayudarán a determinar residuos más simples cuando los que tenemos no son bastante idóneos. *Primero,* si el número ak^2 que es divisible por el cuadrado k^2 (que es relativamente primo a M) es un residuo de M, a será también un residuo. Por esta razón, residuos que son divisibles por cuadrados grandes son precisamente tan útiles como los residuos pequeños, y suponemos que todos los factores cuadrados se han eliminado de todos los residuos suministrados por los siguientes métodos. *Segundo,* si dos o más números son residuos, su producto también será un residuo. Combinando esta observación con la precedente, a menudo puede deducirse, de varios residuos que no son todos lo bastante simples, otro que es simple, con tal que los residuos tengan una gran cantidad de factores comunes. Por esta razón es muy útil tener residuos compuestos de muchos factores que no sean demasiado grandes, y todos ellos serían inmediatamente resueltos en sus factores. La fuerza de estas observaciones será mejor entendida mediante ejemplos y el uso frecuente que mediante reglas.

I. El método más simple y el más conveniente, para aquéllos que han adquirido alguna destreza a través del ejercicio frecuente, consiste en descomponer M o más generalmente un múltiplo de M en dos partes, $kM = a + b$ (ambas partes pueden ser positivas o una positiva y la otra negativa). El producto de estas dos tomado con el signo opuesto será un residuo de M; pues $-ab \equiv a^2 \equiv b^2 \pmod{M}$ y así $-ab \mathrm{R} M$. Los números a y b deben ser tomados de modo que su producto sea divisible por un cuadrado grande y su cociente sea pequeño o al menos resoluble en factores que no sean demasiado grandes, algo que siempre puede hacerse sin dificultad. Se recomienda especialmente que a sea un cuadrado o el doble de un cuadrado o el triple de un cuadrado, etc., el cual difiera de M por un número pequeño o al menos por un número que pueda ser resuelto en factores apropiados. Así, e.g., $997331 = 999^2 - 2\cdot 5\cdot 67 = 994^2 + 5\cdot 11\cdot 13^2 = 2\cdot 706^2 + 3\cdot 17\cdot 3^2 = 3\cdot 575^2 + 11\cdot 31\cdot 4^2 = 3\cdot 577^2 - 7\cdot 13\cdot 4^2 = 3\cdot 578^2 - 7\cdot 19\cdot 37 = 11\cdot 299^2 + 2\cdot 3\cdot 5\cdot 29\cdot 4^2 = 11\cdot 301^2 + 5\cdot 12^2$ etc. Así tenemos los siguientes residuos: $2\cdot 5\cdot 67$, $-5\cdot 11$, $-2\cdot 3\cdot 17$, $-3\cdot 11\cdot 31$, $3\cdot 7\cdot 13$, $3\cdot 7\cdot 19\cdot 37$, $-2\cdot 3\cdot 5\cdot 11\cdot 29$. La última descomposición produce el residuo $-5\cdot 11$ el cual ya tenemos. Para los residuos $-3\cdot 11\cdot 31$, $-2\cdot 3\cdot 5\cdot 11\cdot 29$ podemos sustituir $3\cdot 5\cdot 31$, $2\cdot 3\cdot 29$ que resulta de su combinación con $-5\cdot 11$.

II. El segundo y tercer método se derivan del hecho que si dos formas binarias

$(A,\ B,\ C)$ y $(A',\ B',\ C')$ del mismo determinante M o $-M$ o más generalmente $\pm kM$ pertenecen al mismo género, los números AA', AC' y $A'C$ son residuos de kM; esto no es difícil de ver ya que cualquier número característico, digamos m, de una forma es también un número característico de la otra, y así mA, mC, mA' y mC' son todos residuos de kM. Si por consiguiente $(a,\ b,\ a')$ es una forma reducida del determinante positivo M o del más general kM, y $(a',\ b',\ a'')$, $(a'',\ b'',\ a''')$, etc. son formas en su período, éstas serán equivalentes a ella y ciertamente contenidas en el mismo género. Los números aa', aa'', aa''', etc. serán todos residuos de M. Se puede computar un gran número de formas en tal período con la ayuda del algoritmo del artículo 187. Ordinariamente los residuos más simples resultan de poner $a = 1$ y se omiten aquellos que tengan factores que son demasiado grandes. Aquí están los inicios de los períodos de las formas $(1,\ 998,\ -1327)$ y $(1,\ 1412,\ -918)$ cuyos determinantes son 997331 y 1994662:

$(\ \ 1, 998, -1327)$	$(\ \ 1, 1412, -918)$
$(-1327, 329, \ \ 670)$	$(\ -918, 1342, \ \ 211)$
$(\ \ 670, 341, -1315)$	$(\ \ 211, 1401, -151)$
$(-1315, 974, \ \ 37)$	$(\ -151, 1317, 1723)$
$(\ \ 37, 987, -626)$	$(\ 1723, 406, -1062)$
$(\ -626, 891, \ \ 325)$	$(-1062, 656, 1473)$
$(\ \ 325, 734, -1411)$	$(\ 1473, 817, -901)$
$(-1411, 677, \ \ 382)$	$(\ -901, 985, 1137)$
$(\ \ 382, 851, -715)$	etc.

Por consiguiente todos los números -1327, 670, etc. son residuos del número 997331; olvidando aquéllos que tengan factores demasiado grandes, tenemos éstos: $2 \cdot 5 \cdot 67$, 37, 13, $-17 \cdot 83$, $-5 \cdot 11 \cdot 13$, $-2 \cdot 3 \cdot 17$, $-2 \cdot 59$, $-17 \cdot 53$; hemos encontrado arriba el residuo $2 \cdot 5 \cdot 67$ así como $-5 \cdot 11$ que resulta de una combinación del tercero y el quinto.

III. Sea C cualquier clase, diferente de la clase principal, de formas de un determinante negativo $-M$ o más generalmente $-kM$ y sea su período $2C$, $3C$, etc. (art. 307). Las clases $2C$, $4C$, etc. pertenecerán al género principal; $3C$, $5C$, etc. al mismo género que C. Si por consiguiente (a, b, c) es la (más simple) forma en C y $(a',\ b',\ c')$ una forma en alguna clase del período, digamos nC, o a' o aa' será un residuo de M según que n sea par o impar (en el primer caso c' será también un residuo, en el último caso ac', ca' y cc' lo serán). El cálculo del período, i.e. de las formas más simples en sus clases, es sorprendentemente fácil cuando a es muy pequeño, especialmente cuando es $= 3$, lo que es siempre permisible cuando

$kM \equiv 2 \pmod 3$. He aquí el inicio del período de la clase que contiene a la forma (3, 1, 332444):

$C\,(\ \ 3,\ \ 1, 332444)$	$6C\,(\ 729, -209, 1428)$
$2C\,(\ \ 9, -2, 110815)$	$7C\,(\ 476,\ \ 209, 2187)$
$3C\,(\ 27,\ \ 7,\ \ 36940)$	$8C\,(1027,\ \ 342, 1085)$
$4C\,(\ 81,\ 34,\ \ 12327)$	$9C\,(\ 932, -437, 1275)$
$5C\,(243,\ 34,\ \ 4109)$	$10C\,(\ 425,\ \ \ 12, 2347)$

Después de eliminar aquéllos que no son útiles, tenemos los residuos $3 \cdot 476$, 1027, 1085, 425 o (removiendo los factores cuadrados) $3 \cdot 7 \cdot 17$, $13 \cdot 79$, $5 \cdot 7 \cdot 31$, 17. Si combinamos juiciosamente éstos con los ocho residuos encontrados en II se encuentran los doce siguientes, $-2 \cdot 3$, 13, $-2 \cdot 7$, 17, 37, -53, $-5 \cdot 11$, 79, -83, $-2 \cdot 59$, $-2 \cdot 5 \cdot 31$ y $2 \cdot 5 \cdot 67$. Los seis primeros son los únicos que usamos en el artículo 331. Si queremos, podemos agregar los residuos 19 y -29, que encontramos en I; los otros incluidos allí son dependientes de los que hemos desarrollado aquí.

333.

El segundo metodo para resolver un número dado M en factores depende de una consideración de los valores de la expresión $\sqrt{-D} \pmod M$, junto con las siguientes observaciones.

I. Cuando M es un número primo o una potencia de un primo (impar y que no divide a D), $-D$ será un residuo o un no residuo de M de acuerdo con que M esté contenido en una forma de los divisores o de los no divisores de $x^2 + D$. En el primer caso la expresión $\sqrt{-D} \pmod M$ tendrá únicamente dos valores diferentes, que serán opuestos.

II. Cuando M es compuesto, es decir, $= pp'p''$, etc., donde los números p, p', p'', etc. son primos (distintos, impares y que no dividen a D) o potencias de tales números: $-D$ será un residuo de M solamente cuando es un residuo de cada uno de los p, p', p'', etc., i.e. cuando todos estos números están contenidos en formas de los divisores de $x^2 + D$. Designando los valores de la expresión $\sqrt{-D}$ según los módulos p, p', p'', etc. respectivamente por $\pm r$, $\pm r'$, $\pm r''$, etc. aparecen todos los valores de la misma expresión según el módulo M al determinar los números que son $\equiv r$ o $\equiv -r$ según p, aquéllos que son $\equiv r'$ o $\equiv -r'$ según p', etc. Su número será $= 2^\mu$, donde μ es el número de factores p, p', p'', etc. Ahora, si estos valores son R, $-R$, R', $-R'$, R'', etc., se ve inmediatamente que $R \equiv R$ según todos los números p, p', p'', etc.,

pero que según cualquiera de ellos no se tiene $R \equiv -R$. Así M será el máximo común divisor de M y $R - R$, y 1 es el máximo común divisor de M y $R + R$; pero dos valores que no son ni idénticos ni opuestos, e.g. R y R', deben ser congruentes según uno o varios de los números p, p', p'', etc. pero no según todos ellos y según los otros tendremos $R \equiv -R'$. Así el producto de los primeros será el máximo común divisor de los números M y $R - R'$, y el producto de los últimos será el máximo común divisor de M y $R + R'$. Se sigue de esto que si encontramos todos los máximos comunes divisores de M con las diferencias entre los valores individuales de la expresión $\sqrt{-D}$ (mod. M) y algún valor dado, su conjunto contendrá los números 1, p, p', p'', etc. y todos los productos de pares y triples, etc. de estos números. *De esta forma, por lo tanto, podrán determinarse los números p, p', p'', etc. de los valores de esa expresión.*

Ahora, ya que el método del artículo 327 reduce estos valores a los valores de expresiones de la forma $\frac{m}{n}$ (mod. M) con el denominador n primo relativo a M, no es necesario, para nuestros propósitos presentes, computarlos. El máximo común divisor del número M y la diferencia entre R y R', que corresponden a $\frac{m}{n}$ y $\frac{m'}{n'}$, será obviamente también el máximo común divisor de los números M y $nn'(R - R')$, o de M y $mn' - m'n$, ya que el último es congruente a $nn'(R - R')$ según el módulo M.

334.

Podemos aplicar las observaciones precedentes a nuestro problema de dos maneras; la primera no sólo decide si el número dado M es primo o compuesto, sino que en el segundo caso da sus factores; la segunda es superior en tanto que ella permite cálculos más rápidos, pero, a menos que se repita una y otra vez, no produce los factores de los números compuestos, sin embargo los distingue de los números primos.

I. Se busca primero un número negativo $-D$ que sea un residuo cuadrático de M; para este fin se pueden usar los métodos dados en I y II del artículo 332. En sí, la selección del residuo es arbitraria, ni hay aquí como en el método precedente ninguna necesidad de que D sea un número pequeño. Pero el cálculo será más corto a medida que el número de clases de formas binarias contenidas en cada género propiamente primitivo del determinante $-D$ sea más pequeño. Por consiguiente será conveniente tomar residuos que estén contenidos entre los 65 enumerados en el artículo 303 si alguno de éstos se halla allí. Así, para $M = 997331$ el residuo -102 será el más idóneo de todos los residuos negativos dados arriba. Aparecen todos los valores diferentes de la expresión $\sqrt{-D}$ (mod. M). Si hay solamente dos (opuestos),

M será de seguro un número primo o una potencia de un primo; si hay varios, digamos 2^μ, M estará compuesto de μ números primos o potencias de primos y estos factores pueden ser encontrados por el método del artículo precedente. Estos factores, ya sean primos o potencias de primos, pueden ser determinados directamente, pero la manera como se encuentran los valores de la expresión $\sqrt{-D}$ indicará todos los primos cuyas potencias dividen a M. Puesto que si M es divisible por el cuadrado de un número primo π, el cálculo de seguro producirá una o más representaciones del número $M = am^2 + 2bmn + cn^2$, en las que el máximo común divisor de los números m y n es π (porque en este caso $-D$ es también un residuo de $\frac{M}{\pi^2}$). Pero cuando no existen representaciones en las cuales m y n tengan un divisor común, ésta es una indicación confiable de que M no es divisible por un cuadrado, y así todos los números p, p', p'', etc. son números primos.

Ejemplo. Por el método dado antes se encuentra que existen cuatro valores de la expresión $\sqrt{-408}$ (mod. 997331) que coinciden con los valores de las expresiones $\pm\frac{1664}{113}$ y $\pm\frac{2824}{3}$; los máximos comunes divisores de 997331 con $3 \cdot 1664 - 113 \cdot 2824$ y $3 \cdot 1664 + 113 \cdot 2824$ o con 314120 y 324104 son 7853 y 127, así $997331 = 127 \cdot 7853$ como antes.

II. Tómese un número negativo $-D$ tal que M está contenido en una forma de los divisores de x^2+D; en sí es arbitrario qué número de este tipo se selecciona, pero es ventajoso tener el número de clases en el género del determinante $-D$ tan pequeño como sea posible. No existe dificultad en encontrar un tal número; puesto que entre cualquier cantidad de números probados aproximadamente existen tantos para los que M está contenido en una forma de los divisores como existen para los cuales M está contenido en una forma de los no divisores. Por consiguiente será conveniente comenzar con los 65 números del artículo 303 (comenzando con los más grandes) y si sucede que ninguno de éstos es idóneo (en general esto sucederá solamente una vez en 16384 casos), podemos pasar a otros en los cuales solamente hay dos clases contenidas en cada género. Entonces se investigarán los valores de la expresión $\sqrt{-D}$ (mod. M) y si alguno se encuentra, los factores de M pueden ser deducidos de él, del mismo modo que antes; pero si no se obtienen valores, es decir, si $-D$ es un no residuo de M, ciertamente M no será número primo ni potencia de un número primo. Si en este caso se desean los factores mismos, habremos de repetir la misma operación, usando otro valor para D o ensayando otro método.

Así, e.g., se encuentra que 997331 está contenido en una forma de los no divisores de $x^2 + 1848$, $x^2 + 1365$, $x^2 + 1320$ pero está contenido en una forma de

los divisores de $x^2 + 840$; para los valores de la expresión $\sqrt{-840}$ (mod. 997331) se encuentran las expresiones $\pm\frac{1272}{163}$ y $\pm\frac{3288}{125}$ y de éstos deducimos los mismos factores que antes. Para más ejemplos consulte los del artículo 328, que muestran primero que $5428681 = 307 \cdot 17863$; segundo que 4272943 es un número primo; tercero, que 997331 está ciertamente compuesto de más de un número primo.

Los límites del presente trabajo nos permite insertar aquí únicamente los principios básicos de cada método de hallazgo de factores; guardaremos para otra ocasión una discusión más detallada, junto con tablas auxiliares y otras ayudas.

Sección Sétima

ECUACIONES QUE DEFINEN SECCIONES DE UN CIRCULO.

335.

Dentro de los espléndidos desarrollos, contribución de los matemáticos modernos, la teoría de las funciones circulares sin duda ocupa uno de los lugares más importantes. A menudo tenemos ocasión, en una variedad de contextos, de referirnos a este notable tipo de cantidad, y no hay parte de la matemática general que no dependa de ella en alguna forma. Ya que los más brillantes matemáticos modernos por su industria y sagacidad la han erigido en una extensiva disciplina, se esperaría firmemente que cualquier parte de la teoría, por no hablar de una parte elemental, debería haber sido significativamente desarrollada. Me refiero a la teoría de funciones trigonométricas correspondientes a arcos que son conmesurables con la circunferencia, i.e., la teoría de polígonos regulares. Solamente una pequeña parte de esta teoría ha sido desarrollada hasta ahora, como la siguiente sección aclarará. Los lectores podrían sorprenderse de encontrar una discusión de este tema en el presente trabajo, el cual trata con una disciplina aparentemente tan diferente; pero el tratamiento mismo hará abundantemente claro que hay una conexión íntima entre este tema y la Aritmética Superior.

Los principios de la teoría que vamos a explicar de hecho se extienden mucho más allá de lo que indicaremos. Por ello, pueden ser aplicados no solamente a funciones circulares sino también a otras funciones trascedentales, e.g., a aquéllas que dependen de la integral $\int \frac{dx}{\sqrt{1-x^4}}$ y también a varios tipos de congruencias. Ya que, sin embargo, estamos preparando un gran trabajo sobre esas funciones trascendentales

y puesto que trataremos congruencias extensamente en la continuación de estas *Disquisitiones*, hemos decidido considerar aquí solamente funciones circulares. Y aún cuando es posible discutirlas en toda su generalidad, la reduciremos al caso más simple en el artículo siguiente, tanto por motivos de brevedad como porque los nuevos principios de esta teoría puedan ser más fácilmente comprendidos.

La discusión se reduce al caso más simple, donde el número de partes en las cuales se corta el círculo es un número primo.

336.

Designando la circunferencia del círculo o cuatro ángulos rectos por P y suponiendo que m y n son enteros y n un producto de los factores relativamente primos a, b, c, etc., el ángulo $A = \frac{mP}{n}$ puede ser reducido por los métodos del artículo 310 a la forma $A = (\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \text{ etc.})P$, y las funciones trigonométricas correspondientes a él pueden ser encontradas por métodos conocidos a partir de los de las partes $\frac{\alpha P}{a}$, $\frac{\beta P}{b}$, etc. De esta forma, ya que se pueden tomar a, b, c, etc. como números primos o potencias de números primos, es suficiente considerar la división del círculo en partes cuyo número es un primo o una potencia de un primo y se obtendrá inmediatamente un polígono de n lados a partir de los polígonos de a, b, c, etc. lados. Sin embargo, restringiremos nuestra discusión al caso en que el círculo es dividido en un número primo (impar) de partes, especialmente por la siguiente razón. Es claro que las funciones circulares correspondientes al ángulo $\frac{mP}{p^2}$ son deducidas de las funciones pertenecientes a $\frac{mP}{p}$ mediante la solución de una ecuación de grado p. Y de éste, por una ecuación del mismo grado podemos derivar las funciones correspondientes a $\frac{mP}{p^3}$ etc. De esta forma, si ya se tiene un polígono de p lados, para determinar un polígono de p^λ lados necesariamente se requerirá la solución de $\lambda - 1$ ecuaciones de grado p. Aún cuando la siguiente teoría puede ser extendida también a este caso, no obstante no podremos evitar tantas ecuaciones de grado p, y no existe manera de reducir su grado si p es primo. Así, e.g., se mostrará abajo que un polígono de 17 lados puede ser contruido geométricamente; pero para obtener un polígono de 289 lados no hay manera de eludir el resolver una ecuación de grado 17.

Ecuaciones para funciones trigonométricas de arcos que son una parte o partes de la circunferencia completa,
reducción de las funciones trigonométricas a las raíces de la ecuación $x^n - 1 = 0$.

337.

Es bien conocido que las funciones trigonométricas de todos los ángulos $\frac{kP}{n}$ donde la k denota en general todos los números 0, 1, 2, $\ldots n-1$, son expresadas por las raíces de ecuaciones de grado n. Los *senos* son las raíces de la ecuación (I):

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{ etc.} \pm \frac{1}{2^{n-1}}nx = 0$$

los *cosenos* son las raíces de la ecuación (II):

$$x^n - \frac{1}{4}nx^{n-2} + \frac{1}{16}\frac{n(n-3)}{1\cdot 2}x^{n-4} - \frac{1}{64}\frac{n(n-4)(n-5)}{1\cdot 2\cdot 3}x^{n-6} + \text{etc.} \pm \frac{1}{2^{n-1}}nx - \frac{1}{2^{n-1}} = 0$$

y las *tangentes* son las raíces de la ecuación (III):

$$x^n - \frac{n(n-1)}{1\cdot 2}x^{n-2} + \frac{n(n-1)(n-2)(n-3)}{1\cdot 2\cdot 3\cdot 4}x^{n-4} - \text{ etc. } \pm nx = 0$$

Estas ecuaciones (que son todas verdaderas para cualquier valor impar de n, y la ecuación II es cierta también para cualquier valor par), poniendo $n = 2m+1$, pueden ser fácilmente reducidas a grado m. Para I y III esto justamente requiere dividir a la izquierda por x y sustituir x^2 por y. De todas formas la ecuación II incluye la raíz $x = 1$ $(= \cos 0)$ y todas las otras son iguales en pares $(\cos\frac{P}{n} = \cos\frac{(n-1)P}{n}$, $\cos\frac{2P}{n} = \cos\frac{(n-2)P}{n}$, etc.); así el lado izquierdo es divisible por $x-1$ y el cociente será un cuadrado. Si extraemos la raíz cuadrada, la ecuación II se reduce a la siguiente:

$$x^m + \frac{1}{2}x^{m-1} - \frac{1}{4}(m-1)x^{m-2} - \frac{1}{8}(m-2)x^{m-3} + \frac{1}{16}\frac{(m-2)(m-3)}{1\cdot 2}x^{m-4} + \frac{1}{32}\frac{(m-3)(m-4)}{1\cdot 2}x^{m-5} - \text{ etc.} = 0$$

Sus raíces serán los cosenos de los ángulos $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, $\ldots$ $\frac{mP}{n}$. Hasta ahora no se ha hecho ninguna reducción más allá de estas ecuaciones para el caso en que n es un número primo.

No obstante, ninguna de estas ecuaciones es tan tratable y tan conveniente para nuestros propósitos como $x^n - 1 = 0$. Sus raíces están íntimamente relacionadas

con las raíces de las anteriores. Esto es, escribiendo por brevedad i para la cantidad imaginaria $\sqrt{-1}$, las raíces de la ecuación $x^n - 1 = 0$ serán

$$\cos\frac{kP}{n} + i\,\mathrm{sen}\,\frac{kP}{n} = r$$

donde para k se debe tomar todos los números 0, 1, 2, $\ldots n-1$. De esta forma, ya que $\frac{1}{r} = \cos\frac{kP}{n} - i\,\mathrm{sen}\,\frac{kP}{n}$, las raíces de la ecuación I serán $\frac{1}{2i}(r - \frac{1}{r})$ o $i\frac{1-r^2}{2r}$; las raíces de la ecuación II, $\frac{1}{2}(r + \frac{1}{r}) = \frac{1+r^2}{2r}$; finalmente las raíces de la ecuación III, $\frac{i(1-r^2)}{1+r^2}$. Por esta razón construiremos nuestra investigación sobre una consideración de la ecuación $x^n - 1 = 0$, asumiendo que n es un número primo impar. Con el fin de no interrumpir el orden de la investigación, consideraremos primero el siguiente lema.

338.

PROBLEMA. *Dada la ecuación*

$$(W)\ldots z^m + Az^{m-1} + \text{ etc.} = 0$$

encontrar la ecuación (W') *cuyas raíces son las* λ*-ésimas potencias de las raíces de la ecuación* (W)*, donde* λ *es un exponente entero positivo dado.*

Solución. Si designamos las raíces de la ecuación W por a, b, c, etc., las raíces de la ecuación W' serán a^λ, b^λ, c^λ, etc. Por un teorema de Newton muy conocido, de los coeficientes de la ecuación W se puede encontrar la suma de cualquier potencia de las raíces a, b, c, etc. Por consiguiente, se buscan las sumas

$$a^\lambda + b^\lambda + c^\lambda + \text{ etc.}, \quad a^{2\lambda} + b^{2\lambda} + c^{2\lambda} + \text{ etc. etc.} \quad \text{hasta} \quad a^{m\lambda} + b^{m\lambda} + c^{m\lambda} + \text{ etc.}$$

y por un procedimiento inverso, de acuerdo con el mismo teorema, pueden ser deducidos los coeficientes de la ecuación W', *Q. E. F.* Al mismo tiempo, es claro que si todos los coeficientes de W son racionales, todos los de W' también lo serán. Por otro método se puede probar que si todos los primeros son enteros, los últimos también serán enteros. No gastaremos más tiempo sobre este teorema aquí, puesto que no es necesario para nuestro propósito.

339.

La ecuación $x^n - 1 = 0$ (siempre con la suposición que n es un número primo impar) tiene solamente una raíz real, $x = 1$; las restantes $n-1$ raíces que están dadas por la ecuación

$$x^{n-1} + x^{n-2} + \text{ etc.} + x + 1 = 0$$

son todas imaginarias ; denotaremos su conjunto por Ω y la función

$$x^{n-1} + x^{n-2} + \text{ etc.} + x + 1 \quad \text{por} \quad X$$

Si por consiguiente r es cualquier raíz en Ω, resulta $1 = r^n = r^{2n}$ etc. y en general $r^{en} = 1$ para cualquier valor entero positivo o negativo de e. Así, si λ y μ son enteros congruentes según n, tendremos $r^\lambda = r^\mu$. Pero si λ y μ son no congruentes según n, entonces r^λ y r^μ serán diferentes, pues en este caso se puede encontrar un entero ν tal que $(\lambda - \mu)\nu \equiv 1 \pmod{n}$, así $r^{(\lambda-\mu)\nu} = r$ y ciertamente $r^{\lambda-\mu}$ no es $= 1$. Es claro que cualquier potencia de r es también una raíz de la ecuación $x^n - 1 = 0$. Por lo tanto, ya que las cantidades $1(= r^0)$, r, r^2, $\ldots r^{n-1}$ son todas diferentes, ellas nos darán todas las raíces de la ecuación $x^n - 1 = 0$ y así los números r, r^2, r^3, $\ldots r^{n-1}$ coincidirán con Ω. Más generalmente, entonces, Ω coincidirá con r^e, r^{2e}, r^{3e}, $\ldots r^{(n-1)e}$, si e es cualquier entero positivo o negativo no divisible por n. Tenemos por lo tanto

$$X = (x - r^e)(x - r^{2e})(x - r^{3e}) \ldots (x - r^{(n-1)e})$$

y de esto

$$r^e + r^{2e} + r^{3e} + \ldots + r^{(n-1)e} = -1$$

y

$$1 + r^e + r^{2e} + \ldots + r^{(n-1)e} = 0$$

Si tenemos dos raíces como r y $\frac{1}{r}$ $(= r^{n-1})$ o en general r^e y r^{-e}, las llamaremos raíces *recíprocas*. Evidentemente el producto de dos factores simples $x - r$ y $x - \frac{1}{r}$ es real y es $= x^2 - 2x\cos\omega + 1$, donde el ángulo ω es igual al ángulo $\frac{P}{n}$ o a algún múltiplo de él.

340.

Por eso, representando una raíz en Ω por r, todas las raíces de la ecuación $x^n - 1 = 0$ se expresan mediante potencias de r y el producto de varias raíces de esta

ecuación puede ser expresado por r^λ de manera que λ es 0 o positivo y $< n$. Por lo tanto, si $\varphi(t, u, v, \ldots)$ designa una función algebraica racional entera de las incógnitas t, u, v, etc., que es una suma de términos de la forma $ht^\alpha u^\beta v^\gamma \ldots$, evidentemente si sustituimos t, u, v, etc. por las raíces de la ecuación $x^n - 1 = 0$, digamos $t = a$, $u = b$, $v = c$, etc., entonces $\varphi(a, b, c, \ldots)$ puede ser reducido a la forma

$$A + A'r + A''r^2 + A'''r^3 + \cdots + A^v r^{n-1}$$

de tal manera que los coeficientes A, A', etc. (algunos de ellos pueden no aparecer y por lo tanto son $= 0$) son cantidades determinadas. Y todos estos coeficientes serán enteros si todos los coeficientes en $\varphi(t, u, v, \ldots)$, i.e., todos los h, son enteros. Si después de esto sustituimos t, u, v ..., por a^2, b^2, c^2, ..., respectivamente, cada término $ht^\alpha u^\beta v^\gamma \ldots$ que ha sido reducido a r^σ se hace ahora $r^{2\sigma}$ y así:

$$\varphi(a^2, b^2, c^2, \ldots) = A + A'r^2 + A''r^4 + A'''r^6 + \cdots + A^v r^{2n-2}$$

y en general para cualquier valor entero de λ,

$$\varphi(a^\lambda, b^\lambda, c^\lambda, \ldots) = A + A'r^\lambda + A''r^{2\lambda} + \cdots + A^v r^{(n-1)\lambda}$$

Esta proposición es muy importante y es fundamental para la discusión siguiente. También se sigue de ello que

$$\varphi(1, 1, 1, \ldots) = \varphi(a^n, b^n, c^n, \ldots) = A + A' + A'' + \cdots + A^v$$

y

$$\varphi(a, b, c, \ldots) + \varphi(a^2, b^2, c^2, \ldots) + \varphi(a^3, b^3, c^3, \ldots) + \ldots + \varphi(a^n, b^n, c^n, \ldots) = nA$$

De aquí, esta suma es entera y divisible por n cuando todos los coeficientes en $\varphi(t, u, v, \ldots)$ son enteros.

Teoria de las raíces de la ecuación $x^n - 1 = 0$ (donde n es primo).
Omitiendo la raíz 1, las restantes (Ω) están en $X = x^{n-1} + x^{n-2} +$ etc. $+x + 1 = 0$.
La funcion X no se puede descomponer en factores con coeficientes racionales.

341.

TEOREMA. *Si la función X es divisible por la función de grado más pequeño*

$$P = x^\lambda + Ax^{\lambda-1} + Bx^{\lambda-2} + \cdots + Kx + L$$

los coeficientes A, B, ... L no pueden ser todos racionales.

Demostración. Sea $X = PQ$ y $\mathfrak{P}$ el conjunto de las raíces de la ecuación $P = 0$, $\mathfrak{Q}$ el conjunto de las raíces de la ecuación $Q = 0$, así que Ω consiste de $\mathfrak{P}$ y $\mathfrak{Q}$ tomados juntos. Además, sea $\mathfrak{R}$ el conjunto de raíces recíprocas de $\mathfrak{P}$, $\mathfrak{S}$ el conjunto de raíces recíprocas de $\mathfrak{Q}$ y sean las raíces que están contenidas en $\mathfrak{R}$, raíces de la ecuación $R = 0$ (esto se convierte en $x^\lambda + \frac{K}{L}x^{\lambda-1} +$ etc. $+ \frac{A}{L}x + \frac{1}{L} = 0$) y sean aquéllas que están contenidas en $\mathfrak{S}$, raíces de la ecuación $S = 0$. Evidentemente si tomamos las raíces $\mathfrak{R}$ y $\mathfrak{S}$ juntas obtenemos el conjunto Ω y $RS = X$. Ahora, distinguimos cuatro casos.

I. Cuando $\mathfrak{P}$ coincide con $\mathfrak{R}$ y consecuentemente $P = R$. En este caso obviamente pares de raíces en $\mathfrak{P}$ serán siempre recíprocas y así P será el producto de $\frac{1}{2}\lambda$ factores dobles de la forma $x^2 - 2x\cos\omega + 1$. Como este factor $= (x - \cos\omega)^2 + \operatorname{sen}\omega^2$, es claro que para cualquier valor real de x, P tiene necesariamente un valor real positivo. Sean $P' = 0$, $P'' = 0$, $P''' = 0$, $\ldots P^\nu = 0$ las ecuaciones cuyas raíces son las potencias cuadradas, cúbicas, cuartas, $\ldots (n-1)$-ésimas de las raíces de $\mathfrak{P}$ respectivamente, y sean p, p', p'', $\ldots p^\nu$ los valores de las funciones P, P', P'', $\ldots P^\nu$, respectivamente, que se obtienen al hacer $x = 1$. Entonces, por lo que se dijo antes, p será una cantidad positiva, y por una razón similar también serán positivos p', p'', etc. Ya que, por consiguiente, p es el valor de la función $(1-t)(1-u)(1-v)$ etc., que es obtenida sustituyendo t, u, v, etc. por las raíces contenidas en $\mathfrak{P}$; p' es el valor de la misma función obtenida al sustituir t, u, v, etc., por los cuadrados de esas raíces; y 0 es su valor cuando $t = 1$, $u = 1$, $v = 1$, etc.: la suma $p + p' + p'' \cdots + p^\nu$ será un entero divisible por n. Además es fácil ver que el producto $PP'P'' \ldots$ será $= X^\lambda$ y así $pp'p'' \ldots = n^\lambda$.

Ahora, si todos los coeficientes en P fueran racionales, todos aquéllos en P', P'', etc. también lo serían, por el artículo 338. Sin embargo, por el artículo 42, todos esos coeficientes tendrían que ser enteros. Así p, p', p'', etc. también deberán ser enteros; como su producto es n^λ y su número es $n-1 > \lambda$, algunos de ellos (al menos $n - 1 - \lambda$) deben ser $= 1$, y los otros iguales a n o a una potencia de n. Y si g de ellos son $= 1$, la suma $p + p' +$ etc. será $\equiv g \pmod{n}$ y así, de seguro, no divisible por n. Así, nuestra suposición es inconsistente.

II. Cuando $\mathfrak{P}$ y $\mathfrak{R}$ no coinciden pero contienen algunas raíces comunes, sea $\mathfrak{T}$ este conjunto y $T = 0$, la ecuación de la cual ellos son las raíces. Entonces T será el máximo común divisor de las funciones P y R (como es claro de la teoría de las ecuaciones). Sin embargo, pares de raíces en $\mathfrak{T}$ serán recíprocas y como fue demostrado antes, no todos los coeficientes en T pueden ser racionales. Pero esto de seguro sucedería si todos los de P, y así también los de R, fueran racionales, como

resulta de la naturaleza de la operación por medio de la cual encontramos el máximo común divisor. Así, nuestra suposición es absurda.

III. Cuando $\mathfrak{Q}$ y $\mathfrak{S}$ coinciden o tienen raíces comunes, se prueba, exactamente de la misma forma, que no todos los coeficientes de Q son racionales; pero ellos serían racionales si todos los de P fueran racionales, y esto es imposible.

IV. Si $\mathfrak{P}$ no tiene raíces en común con $\mathfrak{R}$ y $\mathfrak{Q}$ ninguna en común con $\mathfrak{S}$, todas las raíces $\mathfrak{P}$ deberían encontrarse necesariamente en $\mathfrak{S}$, y todas las raíces $\mathfrak{Q}$ en $\mathfrak{R}$. Por lo tanto $P = S$ y $Q = R$, y así $X = PQ$ será el producto de P por R; i.e.,

$$\text{de} \qquad x^\lambda + Ax^{\lambda-1} \cdots + Kx + L \qquad \text{por} \qquad x^\lambda + \frac{K}{L}x^{\lambda-1} \cdots + \frac{A}{L}x + \frac{1}{L}$$

Así, haciendo $x = 1$, resulta

$$nL = (1 + A \ldots + K + L)^2$$

Ahora, si todos los coeficientes en P fueran racionales, y así por el artículo 42 también enteros, L, el cual debe dividir al último coeficiente en X, i.e., la unidad, será necesariamente $= \pm 1$ y así $\pm n$ sería un cuadrado. Pero ya que esto es contrario a la hipótesis, la suposición es inconsistente.

Entonces, por este teorema es claro que no importa como se factorice X, algunos de los coeficientes, al menos, serán irracionales, y así, no se pueden determinar excepto mediante una ecuación de grado mayor que la unidad.

Declaración del propósito de las investigaciones siguientes.

342.

No será inútil declarar en pocas palabras el propósito de las investigaciones siguientes. Es resolver *gradualmente* la X en más y más factores, de manera que sus coeficientes sean determinados por ecuaciones de un orden tan pequeño como sea posible, hasta llegar finalmente a factores simples o sea a las raíces Ω. Probaremos que si el número $n - 1$ es resuelto de alguna manera en factores enteros α, β, γ, etc. (se puede asumir cada uno de ellos primo), X se puede resolver en α factores de grado $\frac{n-1}{\alpha}$ con coeficientes determinados por una ecuación de grado α; cada uno de éstos será resuelto en otros β de grado $\frac{n-1}{\alpha\beta}$ con la ayuda de una ecuación de grado β etc. Así, si ν designa el número de factores α, β, γ, etc., la determinación de las raíces Ω se reduce a la solución de ν ecuaciones de grados α, β, γ, etc. Por ejemplo, para

$n = 17$, donde $n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$, habrá que resolver cuatro ecuaciones cuadráticas; para $n = 73$, tres ecuaciones cuadráticas y dos cúbicas.

En lo que sigue a menudo hay que considerar potencias de la raíz r cuyos exponentes son también potencias: expresiones de esta clase son muy difíciles de imprimir. Por lo tanto, para facilitar la tipografía utilizaremos la siguiente abreviación. Para r, r^2, r^3, etc. escribiremos [1], [2], [3], etc. y en general para r^λ, donde λ es cualquier entero, escribiremos $[\lambda]$. Tales expresiones no están completamente determinadas, pero lo estarán tan pronto como tomemos una raíz específica de Ω para r o sea para [1]. En general $[\lambda]$ y $[\mu]$ serán iguales o diferentes de acuerdo con que λ y μ sean congruentes o no congruentes según el módulo n. Además $[0] = 1$; $[\lambda] \cdot [\mu] = [\lambda + \mu]$; $[\lambda]^v = [\lambda v]$; la suma $[0] + [\lambda] + [2\lambda] \ldots + [(n-1)\lambda]$ es 0 o n de acuerdo con que λ sea no divisible o divisible por n.

Todas las raíces de Ω se distribuyen en ciertas clases (períodos).

343.

Si, para el módulo n, g es ese tipo de número que en la sección III llamamos una raíz primitiva, los $n-1$ números 1, g, g^2, $\ldots g^{n-2}$ serán congruentes a los números 1, 2, 3, $\ldots n-1$ según el módulo n. El orden será diferente, pero todo número en una serie será congruente a alguno en la otra. De esto se sigue inmediatamente que las raíces [1], [g], [g^2], $\ldots$ [g^{n-2}] coinciden con Ω. Por un argumento similar las raíces

$$[\lambda],\ [\lambda g],\ [\lambda g^2],\ \ldots\ [\lambda g^{n-2}]$$

coincidirán con Ω cuando λ es cualquier entero no divisible por n. Además, ya que $g^{n-1} \equiv 1 \pmod{n}$, es fácil ver que las dos raíces $[\lambda g^\mu]$ y $[\lambda g^\nu]$ serán identicas o diferentes de acuerdo con que μ y ν sean congruentes o no congruentes según $n - 1$.

Si por lo tanto G es otra raíz primitiva, las raíces [1], [g], $\ldots$ [g^{n-2}] también coincidirán con [1], [G], $\ldots$ [G^{n-2}], exceptuando el orden. Además, si e es un divisor de $n - 1$, y se pone $n - 1 = ef$, $g^e = h$, $G^e = H$, entonces los f números 1, h, h^2, $\ldots h^{f-1}$ serán congruentes a 1, H, H^2, $\ldots H^{f-1}$ según n (sin considerar el orden). Supongamos que $G \equiv g^\omega \pmod{n}$, que μ es un número positivo arbitrario $< f$ y que ν es el residuo más pequeño de $\mu\omega \pmod{f}$. Entonces resultará $\nu e \equiv \mu\omega e \pmod{n-1}$ y así $g^{\nu e} \equiv g^{\mu\omega e} \equiv G^{\mu e} \pmod{n}$ o $H^\mu \equiv h^\nu$; i.e., cualquier número en la segunda serie 1, H, H^2, etc. será congruente a un número en la serie 1, h, h^2, $\ldots$

y viceversa. Así, las f raíces [1], [h], [h^2], ... [h^{f-1}] serán idénticas con [1], [H], [H^2], ... [H^{f-1}]. De la misma manera, es fácil ver que las series más generales

$$[\lambda], [\lambda h], [\lambda h^2], \ldots [\lambda h^{f-1}] \quad \text{y} \quad [\lambda], [\lambda H], [\lambda H^2], \ldots [\lambda H^{f-1}]$$

coinciden. Designaremos la *suma* de tales f raíces, $[\lambda] + [\lambda h] +$ etc. $+ [\lambda h^{f-1}]$ por (f, λ). Puesto que ella no cambia al tomar una raíz primitiva diferente g, debe ser considerada como independiente de g. Llamaremos al *conjunto* de las mismas raíces el *período* (f, λ) y olvidaremos el orden de las raíces *). Para exhibir un tal período será conveniente reducir cada raíz a su expresión más simple, esto es, sustituir los números λ, λh, λh^2, etc. por sus residuos más pequeños según el módulo n. Se podrían ordenar los términos de acuerdo con los tamaños de estos residuos.

Por ejemplo, para $n = 19$, 2 es una raíz primitiva y su período (6,1) consiste de las raíces [1], [8], [64], [512], [4096] y [32768] o sea [1], [7], [8], [11], [12] y [18]. Similarmente, el período (6,2) consiste de las raíces [2], [3], [5], [14], [16] y [17]. El período (6,3) es idéntico con el precedente. El período (6,4) contiene las raíces [4], [6], [9], [10], [13] y [15].

Varios teoremas concernientes a estos períodos.

344.

Se ofrecen inmediatamente las siguientes observaciones acerca de períodos de este tipo.

I. Ya que $\lambda h^f \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h$, etc. (mod. n), es claro que (f, λ), $(f, \lambda h)$, $(f, \lambda h^2)$, etc. están compuestos por las mismas raíces. En general, por consiguiente, si designamos por $[\lambda']$ cualquier raíz en (f, λ), este período será completamente idéntico a (f, λ'). Si por lo tanto dos períodos que tienen el mismo número de raíces (los llamaremos *similares*) tienen una raíz en común, ellos serán idénticos. Por lo tanto no puede ocurrir que dos raíces estén contenidas juntas en un período y solamente una de ellas se encuentre en otro período similar. Además, si dos raíces $[\lambda]$ y $[\lambda']$ pertenecen al mismo período de f términos, el valor de la expresión $\frac{\lambda'}{\lambda}$ (mod. n) es congruente a alguna potencia de h; esto es, podemos asumir que $\lambda' \equiv \lambda g^{\nu e}$ (mod. n).

II. Si $f = n - 1$, $e = 1$, el período $(f, 1)$ coincidirá con Ω. En los casos restantes Ω estará compuesto por los períodos $(f, 1)$, (f, g), (f, g^2), ... (f, g^{e-1}). Por

*) En lo que sigue también es posible llamar a la suma el valor numérico del período, o simplemente el período, cuando no haya ambigüedad.

lo tanto estos períodos serán completamente diferentes unos de otros y es claro que cualquier otro período similar (f, λ) coincidirá con uno de éstos si $[\lambda]$ pertenece a Ω, i.e., si λ no es divisible por n. El período $(f, 0)$ o (f, kn) está evidentemente compuesto de f unidades. También es claro que si λ es cualquier número no divisible por n, el conjunto de e períodos (f, λ), $(f, \lambda g)$, $(f, \lambda g^2)$, $\ldots (f, \lambda g^{e-1})$ también coincidirá con Ω. Así, e.g., para $n = 19$, $f = 6$, Ω consistirá de los tres períodos (6,1), (6,2) y (6,4). Cualquiera otro período similar, excepto (6,0), puede ser reducido a uno de éstos.

III. Si $n - 1$ es el producto de tres números positivos a, b y c, es evidente que cualquier período de bc términos está compuesto de b períodos de c términos; por ejemplo (bc, λ) está compuesto por (c, λ), $(c, \lambda g^a)$, $(c, \lambda g^{2a}) \ldots (c, \lambda g^{ab-a})$. Estos últimos se dicen estar contenidos en los primeros. Así para $n = 19$ el período (6,1) consiste de los tres períodos (2,1), (2,8) y (2,7). El primero contiene las raíces r y r^{18}; el segundo r^8 y r^{11}; el tercero r^7 y r^{12}.

345.

Teorema. *Sean (f, λ) y (f, μ) dos períodos similares, idénticos o diferentes, (f, λ) consistiendo de las raíces $[\lambda]$, $[\lambda']$, $[\lambda'']$, etc. Entonces el producto de (f, λ) por (f, μ) será la suma de f períodos similares, a saber*

$$= (f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \text{ etc.} = W$$

Demostración. Sea como antes $n - 1 = ef$; g una raíz primitiva para el módulo n y $h = g^e$. De lo que hemos dicho antes, tenemos $(f, \lambda) = (f, \lambda h) = (f, \lambda h^2)$ etc. El producto buscado será

$$= [\mu] \cdot (f, \lambda) + [\mu h] \cdot (f, \lambda h) + [\mu h^2] \cdot (f, \lambda h^2) + \text{ etc.}$$

y así

$$\begin{array}{llll} = [\lambda + \mu] & +[\lambda h + \mu] & \cdots & +[\lambda h^{f-1} + \mu] \\ +[\lambda h + \mu h] & +[\lambda h^2 + \mu h] & \cdots & +[\lambda h^f + \mu h] \\ +[\lambda h^2 + \mu h^2] & +[\lambda h^3 + \mu h^2] & \cdots & +[\lambda h^{f+1} + \mu h^2] \text{ etc.} \end{array}$$

una expresión que contendrá en conjunto f^2 raíces. Y si se suman las columnas verticales juntas, resulta

$$(f, \lambda + \mu) + (f, \lambda h + \mu) + \cdots + (f, \lambda h^{f-1} + \mu)$$

una expresión que coincide con W, porque por hipótesis los números λ, λ', λ'', etc. son congruentes a λ, λh, λh^2, $\ldots \lambda h^{f-1}$ según el módulo n (aquí no estamos interesados en el orden) y así también

$$\lambda + \mu, \quad \lambda' + \mu, \quad \lambda'' + \mu, \quad \text{etc.}$$

serán congruentes a

$$\lambda + \mu, \quad \lambda h + \mu, \quad \lambda h^2 + \mu, \quad \ldots \ \lambda h^{f-1} + \mu \quad \textit{Q. E. D.}$$

Agregamos los siguientes corolarios a este teorema:

I. Si k designa cualquier entero, el producto de $(f, k\lambda)$ por $(f, k\mu)$ será

$$= (f, k(\lambda + \mu)) + (f, k(\lambda' + \mu)) + (f, k(\lambda'' + \mu)) + \text{ etc.}$$

II. Ya que los términos particulares de W coinciden con la suma $(f, 0)$ la cual $= f$, o con una de las sumas $(f, 1)$, (f, g), $(f, g^2) \ldots (f, g^{e-1})$, W puede ser reducido a la siguiente forma

$$W = af + b(f, 1) + b'(f, g) + b''(f, g^2) + \cdots + b^{\varepsilon}(f, g^{e-1})$$

donde los coeficientes a, b, b', etc. son enteros positivos (o alguno puede aún ser $= 0$). Es también claro que el producto de $(f, k\lambda)$ por $(f, k\mu)$ entonces se convertirá en

$$= af + b(f, k) + b'(f, kg) + \cdots + b^{\varepsilon}(f, kg^{e-1})$$

Así, e.g., para $n = 19$ el producto de la suma $(6, 1)$ por ella misma, o sea el cuadrado de esta suma, será $= (6, 2) + (6, 8) + (6, 9) + (6, 12) + (6, 13) + (6, 19) = 6 + 2(6, 1) + (6, 2) + 2(6, 4)$.

III. Puesto que el producto de los términos individuales de W por un período similar (f, ν) puede ser reducido a una forma análoga, es evidente que el producto de tres períodos $(f, \lambda) \cdot (f, \mu) \cdot (f, \nu)$ puede ser representado por $cf + d(f, 1) \ldots + d^{\varepsilon}(f, g^{e-1})$ y los coeficientes c, d, etc. serán enteros y positivos (o $= 0$) y para cualquier valor entero de k tenemos

$$(f, k\lambda) \cdot (f, k\mu) \cdot (f, k\nu) = cf + d(f, k) + d'(f, kg) + \text{ etc.}$$

Este teorema puede ser extendido al producto de cualquier número de períodos similares, y no importa si estos períodos son todos diferentes o parcialmente o totalmente idénticos.

IV. Se sigue de esto que si en cualquier función algebraica racional entera $F = \varphi(t, u, v, \ldots)$ sustituimos las incógnitas t, u, v, etc. por los períodos similares (f, λ), (f, μ), (f, ν), etc. respectivamente, su valor será reducible a la forma

$$A + B(f, 1) + B'(f, g) + B''(f, g^2) \cdots + B^{\varepsilon}(f, g^{e-1})$$

y los coeficientes A, B, B', etc. serán enteros si todos los coeficientes en F son enteros. Pero si después sustituimos t, u, v, etc. por $(f, k\lambda)$, $(f, k\mu)$, $(f, k\nu)$, etc. respectivamente, el valor de F será reducido a $A + B(f, k) + B'(f, kg) +$ etc.

346.

TEOREMA. *Suponiendo que λ es un número no divisible por n, y escribiendo por brevedad p en lugar de (f, λ), cualquier otro período similar (f, μ), en el cual μ no es divisible por n, puede ser reducido a la forma*

$$\alpha + \beta p + \gamma p^2 + \cdots + \theta p^{e-1}$$

donde los coeficientes α, β, etc. son cantidades racionales determinadas.

Demostración. Desígnense por p', p'', p''', etc. los períodos $(f, \lambda g)$, $(f, \lambda g^2)$, $(f, \lambda g^3)$, etc. hasta $(f, \lambda g^{e-1})$. Su número será $e - 1$ y uno de ellos necesariamente coincidirá con (f, μ). Inmediatamente resulta la ecuación

$$0 = 1 + p + p' + p'' + p''' + \text{ etc.} \qquad (I)$$

Ahora, si de acuerdo con las reglas del artículo precedente se desarrollan las potencias de p hasta la $e - 1$-ésima, se extenderán otras $e - 2$ ecuaciones

$$0 = p^2 + A + ap + a'p' + a''p'' + a'''p''' + \text{ etc.} \qquad (II)$$
$$0 = p^3 + B + bp + b'p' + b''p'' + b'''p''' + \text{ etc.} \qquad (III)$$
$$0 = p^4 + C + cp + c'p' + c''p'' + c'''p''' + \text{ etc.} \qquad (IV)$$
$$\text{etc.}$$

Todos los coeficientes A, a, a', etc.; B, b, b', etc.; etc. serán enteros y, como sigue inmediatamente del artículo precedente, completamente independientes de λ; esto es, se obtienen las mismas ecuaciones no importa cual sea el valor que demos a λ. Esta observación puede ser extendida a la ecuación I en tanto que λ no sea divisible por n. Supongamos que $(f, \mu) = p'$; por ello es fácil ver que si (f, μ) coincide con cualquiera de los otros períodos p'', p''', etc. la siguiente línea de argumento puede ser usada de modo completamente análogo. Ya que el número de ecuaciones I, II, III, etc. es $e-1$, las cantidades p'', p''', etc. cuyo número es $= e-2$, pueden ser eliminadas de ellas por métodos conocidos. La ecuación resultante (Z) estará libre de ellas:

$$0 = \mathfrak{A} + \mathfrak{B}p + \mathfrak{C}p^2 + \text{ etc.} + \mathfrak{M}p^{e-1} + \mathfrak{N}p'$$

Esto se puede hacer de manera tal que todos los coeficientes $\mathfrak{A}$, $\mathfrak{B}$, $\ldots\,\mathfrak{N}$ sean enteros y de seguro no todos $= 0$. Ahora, si no tenemos $\mathfrak{N} = 0$, se sigue que p' puede ser determinado como lo demanda el teorema. Queda por lo tanto probar que no puede hacerse $\mathfrak{N} = 0$.

Suponiendo que $\mathfrak{N} = 0$, la ecuación Z se convierte en $\mathfrak{M}p^{e-1} + \text{etc.} + \mathfrak{B}p + \mathfrak{A} = 0$. Ya que ella no puede tener grado mayor que $e-1$, no es satisfecha por más que $e-1$ valores diferentes de p. Pero ya que las ecuaciones de las cuales se deduce Z son independientes de λ, se sigue que Z no depende de λ y así ella tendrá lugar, no importa qué entero no divisible por n tomemos para λ. Por consiguiente esta ecuación Z será satisfecha por cualquiera de las sumas $(f, 1)$, (f, g), (f, g^2), $\ldots\,(f, g^{e-1})$, y se sigue inmediatamente que no todas estas sumas pueden ser diferentes sino que al menos dos de ellas deben ser iguales. Suponga que una de estas dos sumas iguales contiene las raíces $[\zeta]$, $[\zeta']$, $[\zeta'']$, etc. y la otra las raíces $[\eta]$, $[\eta']$, $[\eta'']$, etc. Supondremos (esto es legítimo) que todos los números ζ, ζ', ζ'', etc., η, η', η'', etc. son positivos y $< n$. Evidentemente todos serán diferentes y ninguno de ellos $= 0$. Designaremos por Y la función

$$x^{\zeta} + x^{\zeta'} + x^{\zeta''} + \text{ etc.} - x^{\eta} - x^{\eta'} - x^{\eta''} - \text{ etc.}$$

Su término mayor no puede exceder a x^{n-1} y $Y = 0$ si se pone $x = [1]$. Así Y tendrá un factor $x - [1]$ en *común* con la función denotada por X en lo que precede y es fácil probar que esto sería absurdo. En efecto, si Y y X tienen un factor común, el máximo común divisor de las funciones X e Y (no puede tener grado $n-1$ porque Y es divisible por x) tendría todos sus coeficientes racionales. Esto seguiría de la

naturaleza de las operaciones involucradas en encontrar el máximo común divisor de dos funciones cuyos coeficientes son todos racionales. Pero en el artículo 341 probamos que X no puede tener un factor con coeficientes racionales de grado menor que $n-1$. Por lo tanto la suposición $\mathfrak{N} = 0$ no puede ser consistente.

Ejemplo. Para $n = 19$, $f = 6$ resulta $p^2 = 6 + 2p + p' + 2p''$. Ya que $0 = 1 + p + p' + p''$, deducimos que $p' = 4 - p^2$, $\quad p'' = -5 - p + p^2$. Por consiguiente

$$\begin{aligned} (6,2) &= 4 - (6,1)^2, \qquad & (6,4) &= -5 - (6,1) + (6,1)^2 \\ (6,4) &= 4 - (6,2)^2, \qquad & (6,1) &= -5 - (6,2) + (6,2)^2 \\ (6,1) &= 4 - (6,4)^2, \qquad & (6,2) &= -5 - (6,4) + (6,4)^2 \end{aligned}$$

347.

TEOREMA. *Sea* $F = \varphi(t, u, v, \ldots)$ *una función algebraica racional entera invariable**) en las incógnitas t, u, v, etc. Sustituyendo éstas por las f raíces contenidas en el período (f, λ), por las reglas del artículo 340 el valor de F es reducido a la forma

$$A + A'[1] + A''[2] + \text{ etc.} = W\,.$$

Entonces las raíces que pertenecen al mismo período de f términos tendrán coeficientes iguales en esta expresión.

Demostración. Sean $[p]$ y $[q]$ dos raíces pertenecientes al mismo período y suponga que p y q son positivas y menores que n. Hay que mostrar que $[p]$ y $[q]$ tienen el mismo coeficiente en W. Sea $q \equiv pg^{\nu e} \pmod{n}$; y sean $[\lambda]$, $[\lambda']$, $[\lambda'']$, etc. las raíces contenidas en (f, λ), donde suponemos que λ, λ', λ'', etc. son positivos y menores que n; finalmente sean μ, μ', μ'', etc. los menores residuos positivos de los números $\lambda g^{\nu e}$, $\lambda' g^{\nu e}$, $\lambda'' g^{\nu e}$, etc. según el módulo n. Evidentemente éstos serán idénticos con los números λ, λ', λ'', etc., aunque el orden puede estar transpuesto. Del artículo 340 es claro que

$$\varphi([\lambda g^{\nu e}], [\lambda' g^{\nu e}], [\lambda'' g^{\nu e}], \ldots) = (I)$$

---

*) Funciones invariables son aquéllas en las que todas las incógnitas están contenidas del mismo modo, o, más claramente, funciones que no cambian no importa la forma en que se presenten las incógnitas; tales son por ejemplo, la suma de las incógnitas, su producto, la suma de productos de pares de ellas, etc.

es reducido a

$$A + A'[g^{\nu e}] + A''[2g^{\nu e}] + \text{ etc.} \quad \text{o a} \quad A + A'[\theta] + A''[\theta'] + \text{ etc.} = (W')$$

Aquí, θ, θ', etc. designan los residuos mínimos de los números $g^{\nu e}$, $2g^{\nu e}$, etc. según el módulo n y así vemos que el coeficiente que tiene $[q]$ en (W') es el mismo que tiene $[p]$ en (W). Si desarrollamos la expresión (I) obtendremos lo mismo que obtenemos de desarrollar la expresión $\varphi([\mu], [\mu'], [\mu'']$, etc.) porque $\mu \equiv \lambda g^{\nu e}$, $\mu' \equiv \lambda' g^{\nu e}$, etc. (mod. n). De hecho, esta última expresión produce el mismo resultado que $\varphi([\lambda], [\lambda'], [\lambda'']$, etc.), ya que los números μ, μ', μ'', etc. difieren de los números λ, λ', λ'', etc. solamente en el orden y esto no tiene importancia en una función invariable. Así, W' es completamente idéntico con W y por eso la raíz $[q]$ tendrá el mismo coeficiente que $[p]$ en W. *Q. E. D.*

Entonces es claro que W puede ser reducido a la forma

$$A + a(f, 1) + a'(f, g) + a''(f, g^2) + \cdots + a^{\varepsilon}(f, g^{e-1})$$

y los coeficientes A, a, $\ldots a^{\varepsilon}$ serán cantidades determinadas y enteras si todos los coeficientes racionales en F son enteros. Así, e.g., si $n = 19$, $f = 6$, $\lambda = 1$ y la función φ designa la suma de los productos de las incógnitas tomadas dos a dos, su valor es reducido a $3 + (6, 1) + (6, 4)$.

Si después de esto t, u, v, etc. son sustituidas por las raíces de otro período $(f, k\lambda)$, el valor de F se convertirá en

$$A + a(f, k) + a'(f, kg) + a''(f, kg^2) + \text{ etc.}$$

348.

En cualquier ecuación

$$x^f - \alpha x^{f-1} + \beta x^{f-2} - \gamma x^{f-3} \cdots = 0$$

los coeficientes α, β, γ, etc. son funciones invariables de las raíces; esto es, α es la suma de todas ellas, β es la suma de sus productos tomados dos a la vez, γ es la suma de sus productos tomados tres a la vez, etc. Por lo tanto en la ecuación cuyas

raíces son aquéllas contenidas en el período (f, λ), el primer coeficiente será $= (f, \lambda)$ y cada uno de los otros puede ser reducido a la forma

$$A + a(f, 1) + a'(f, g) + \cdots + a^{\varepsilon}(f, g^{e-1})$$

con todos los A, a, a', etc. enteros. Es luego evidente que la ecuación cuyas raíces son las raíces contenidas en cualquiera otro período $(f, k\lambda)$ puede ser derivada de la anterior sustituyendo $(f, 1)$ por (f, k) en cada uno de los coeficientes, (f, g) por (f, kg), y en general (f, p) por (f, kp). De esta forma por lo tanto, se pueden especificar e ecuaciones $z = 0$, $z' = 0$, $z'' = 0$, etc., cuyas raíces serán las raíces contenidas en $(f, 1)$, (f, g), (f, g^2), etc., tan pronto como encontremos las e sumas $(f, 1)$, (f, g), (f, g^2), etc. o mejor dicho tan pronto como encontremos *una* cualquiera de ellas. Esto es cierto porque, por el artículo 346, todas las restantes pueden ser deducidas racionalmente de una de ellas. Hecho esto, la función X será resuelta en e factores de grado f, pues evidentemente el producto de las funciones z, z', z'', etc. será $= X$.

Ejemplo. Para $n = 19$ la suma de todas las raíces en el período $(6, 1)$ es $(6, 1) = \alpha$; la suma de sus productos tomados dos a la vez $= 3 + (6, 1) + (6, 4) = \beta$; similarmente, la suma de los productos tomados tres a la vez $= 2+2(6, 1)+(6, 2) = \gamma$; la suma de los productos tomados cuatro a la vez $= 3 + (6, 1) + (6, 4) = \delta$; la suma de los productos tomados cinco a la vez $= (6, 1) = \varepsilon$; el producto de todos ellos $= 1$. Así la ecuación

$$z = x^6 - \alpha x^5 + \beta x^4 - \gamma x^3 + \delta x^2 - \varepsilon x + 1 = 0$$

contendrá todas las raíces incluidas en $(6, 1)$. Y si sustituimos $(6, 1)$, $(6, 2)$ y $(6, 4)$ por $(6, 2)$, $(6, 4)$ y $(6, 1)$ respectivamente en los coeficientes α, β, γ, etc., resultará la ecuación $z' = 0$, la cual contendrá las raíces de $(6, 2)$. Si la misma permutación se aplica de nuevo, tendremos la ecuación $z'' = 0$ conteniendo las raíces de $(6, 4)$, y el producto $zz'z'' = X$.

349.

A menudo es más conveniente, en especial cuando f es un número grande, deducir los coeficientes β, γ, etc. de las sumas de las potencias de las raíces, por el teorema de Newton. Así la suma de los cuadrados de las raíces contenidas en (f, λ)

es $= (f, 2\lambda)$, la suma de los cubos es $= (f, 3\lambda)$, etc. Si escribimos q, q', q'', etc. por (f, λ), $(f, 2\lambda)$, $(f, 3\lambda)$, etc. tendremos

$$\alpha = q, \qquad 2\beta = \alpha q - q', \qquad 3\gamma = \beta q - \alpha q' + q'', \quad \text{etc.}$$

donde, por el artículo 345, el producto de dos períodos ha de ser convertido inmediatamente en una suma de períodos. Así, en nuestro ejemplo, escribiendo p, p' y p'' por $(6, 1)$, $(6, 2)$ y $(6, 4)$ respectivamente, tendremos q, q', q'', q''', q'''' y q''''' respectivamente $= p$, p', p', p'', p' y p''. Luego

$$\alpha = p, \qquad 2\beta = p^2 - pp' = 6 + 2p + 2p''$$
$$3\gamma = (3 + p + p'')p - pp' + p' = 6 + 6p + 3p'$$
$$4\delta = (2 + 2p + p')p - (3 + p + p'')p' + pp' - p'' = 12 + 4p + 4p'', \text{ etc.}$$

Sin embargo, es suficiente computar la mitad de los coeficientes de esta manera, porque no es difícil probar que los últimos son iguales a los primeros en orden inverso; esto es, el último $= 1$, el penúltimo $= \alpha$, el antepenúltimo $= \beta$, etc.; o, de otra manera, el último puede ser derivado del primero sustituyendo $(f, 1)$, (f, g), etc. por los períodos $(f, -1)$, $(f, -g)$, etc. o sea $(f, n-1)$, $(f, n-g)$, etc. Los primeros casos se tienen cuando f es impar. El último coeficiente, sin embargo, siempre será $= 1$. La base para esto es establecida por el teorema del artículo 79, pero por razones de brevedad no nos dilataremos en el argumento.

350.

Teorema. *Sea $n-1$ el producto de los tres enteros positivos α, β y γ y considere el período $(\beta\gamma, \lambda)$ de $\beta\gamma$ términos compuesto de los β períodos menores de γ términos, (γ, λ), (γ, λ'), (γ, λ''), etc. Supongamos luego que en una función de β incógnitas tal como en el artículo* 347, *esto es en $F = \varphi(t, u, v, \ldots)$, se sustituyen las incógnitas t, u, v, etc. por las sumas (γ, λ), (γ, λ'), (γ, λ''), etc. respectivamente y de acuerdo con las reglas del artículo* 345.IV *su valor es reducido a*

$$A + a(\gamma, 1) + a'(\gamma, g) \cdots + a^{\zeta}(\gamma, g^{\alpha\beta-\alpha}) \cdots + a^{\theta}(\gamma, g^{\alpha\beta-1}) = W$$

Entonces digo que si F es una función invariable, los períodos en W que están contenidos en el mismo período de $\beta\gamma$ términos (i.e. en general los períodos (γ, g^{μ}) y $(\gamma, g^{\alpha\nu+\mu})$ donde ν es cualquier entero), tendrán los mismos coeficientes.

Demostración. Ya que el período $(\beta\gamma, \lambda g^\alpha)$ es idéntico a $(\beta\gamma, \lambda)$, los períodos menores $(\gamma, \lambda g^\alpha)$, $(\gamma, \lambda' g^\alpha)$, $(\gamma, \lambda'' g^\alpha)$, etc. los cuales comprenden al primero, necesariamente coinciden con aquéllos que comprenden al último, aunque en un orden diferente. Si se supone que F será transformado en W' sustituyendo t, u, v, etc. por las primeras cantidades, respectivamente, W' coincidirá con W. Pero por el artículo 347 resulta

$$\begin{aligned} W' &= A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) \cdots + a^\zeta(\gamma, g^{\alpha\beta}) \cdots + a^\theta(\gamma, g^{\alpha\beta+\alpha-1}) \\ &= A + a(\gamma, g^\alpha) + a'(\gamma, g^{\alpha+1}) \cdots + a^\zeta(\gamma, 1) \cdots + a^\theta(\gamma, g^{\alpha-1}) \end{aligned}$$

así esta expresión debe coincidir con W y el primero, segundo, tercero, etc. coeficientes en W (comenzando con a) deben coincidir con el $\alpha+1$-ésimo, el $\alpha+2$-ésimo, el $\alpha+3$-ésimo, etc. Concluimos en general que los coeficientes de los períodos (γ, g^μ), $(\gamma, g^{\alpha+\mu})$, $(\gamma, g^{2\alpha+\mu})$, $\ldots (\gamma, g^{\nu\alpha+\mu})$, los cuales son el $\mu-1$-ésimo, el $\alpha+\mu+1$-ésimo, el $2\alpha+\mu+1$-ésimo, $\ldots \nu\alpha+\mu+1$-ésimo $\ldots$ deben coincidir con alguno otro. *Q. E. D.*

Así, es claro que W puede ser reducido a la forma

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \cdots + a^\varepsilon(\beta\gamma, g^{\alpha-1})$$

con todos los coeficientes A, a, etc. enteros, si todos los coeficientes en F son enteros. Suponga después de esto que sustituimos las incógnitas en F por los β períodos de γ términos que constituyen otro período de $\beta\gamma$ términos, por ejemplo, aquéllos contenidos en $(\beta\gamma, \lambda k)$ que son $(\gamma, \lambda k)$, $(\gamma, \lambda' k)$, $(\gamma, \lambda'' k)$, etc. Entonces el valor resultante será $A + a(\beta\gamma, k) + a'(\beta\gamma, gk) \cdots + a^\varepsilon(\beta\gamma, g^{\alpha-1}k)$.

Es obvio que el teorema puede ser extendido al caso donde $\alpha = 1$ o $\beta\gamma = n-1$. En este caso *todos* los coeficientes en W serán iguales, y W será reducido a la forma $A + a(\beta\gamma, 1)$.

351.

Ahora, reteniendo la terminología del artículo precedente, es claro que los coeficientes individuales de la ecuación cuyas raíces son las β sumas (γ, λ), (γ, λ'), (γ, λ''), etc. pueden ser reducidos a una forma como

$$A + a(\beta\gamma, 1) + a'(\beta\gamma, g) \cdots + a^\varepsilon(\beta\gamma, g^{\alpha-1})$$

y los números A, a etc. serán todos enteros. Se deriva de esto la ecuación cuyas raíces son los β períodos de γ términos contenidos en otro período $(\beta\gamma, k\lambda)$ si en todos los

coeficientes sustituimos todos los períodos $(\beta\gamma, \mu)$ por $(\beta\gamma, k\mu)$. Si por consiguiente $\alpha = 1$, todos los β períodos de γ términos estarán determinados por una ecuación de grado β, y cada uno de los coeficientes será de la forma $A + a(\beta\gamma, 1)$. Como resultado, *todos ellos serán cantidades conocidas* porque $(\beta\gamma, 1) = (n-1, 1) = -1$. Si $\alpha > 1$, los coeficientes de la ecuación cuyas raíces son todos los períodos de γ términos contenidos en un período dado de $\beta\gamma$ términos, serán cantidades conocidas en tanto que todos los valores numéricos de todos los α períodos de $\beta\gamma$ términos sean conocidos. El cálculo de los coeficientes de estas ecuaciones será a menudo más fácil, especialmente cuando β no es muy pequeño, si primero se calculan las sumas de las potencias de las raíces y se deducen de éstas los coeficientes por el teorema de Newton, como arriba en el artículo 349.

Ejemplo. I. Para $n = 19$ se busca la ecuación cuyas raíces son las sumas $(6, 1)$, $(6, 2)$ y $(6, 4)$. Designando estas raíces por p, p', p'', etc. respectivamente y la ecuación buscada por

$$x^3 - Ax^2 + Bx - C = 0$$

tenemos

$$A = p + p' + p'', \qquad B = pp' + pp'' + p'p'', \qquad C = pp'p''$$

Entonces

$$A = (18, 1) = -1$$

y

$$pp' = p + 2p' + 3p'', \qquad pp'' = 2p + 3p' + p'', \qquad p'p'' = 3p + p' + 2p''$$

así

$$B = 6(p + p' + p'') = 6(18, 1) = -6$$

y finalmente

$$C = (p + 2p' + 3p'')p'' = 3(6, 0) + 11(p + p' + p'') = 18 - 11 = 7$$

por lo tanto la ecuación buscada es

$$x^3 + x^2 - 6x - 7 = 0$$

Usando el otro método, tenemos

$$p + p' + p'' = -1$$

$$p^2 = 6 + 2p + p' + 2p'', \qquad p'^2 = 6 + 2p' + p'' + 2p, \qquad p''^2 = 6 + 2p'' + p + 2p'$$

de donde

$$p^2 + p'^2 + p''^2 = 18 + 5(p + p' + p'') = 13$$

y similarmente

$$p^3 + p'^3 + p''^3 = 36 + 34(p + p' + p'') = 2$$

De esto y del teorema de Newton derivamos la misma ecuación que antes.

II. Para $n = 19$ se busca la ecuación cuyas raíces son las sumas $(2, 1)$, $(2, 7)$ y $(2, 8)$. Si las designamos por q, q' y q'' encontramos

$$q + q' + q'' = (6, 1), \qquad qq' + qq'' + q'q'' = (6, 1) + (6, 4), \qquad qq'q'' = 2 + (6, 2)$$

y así, reteniendo la misma notación que en lo precedente, la ecuación buscada será

$$x^3 - px^2 + (p + p'')x - 2 - p' = 0$$

La ecuación cuyas raíces son las sumas $(2, 2)$, $(2, 3)$ y $(2, 5)$ contenidas en $(6, 2)$ puede ser deducida de lo anterior sustituyendo p, p' y p'' por p', p'' y p, respectivamente, y si hacemos la misma sustitución nuevamente, se obtiene la ecuación cuyas raíces son las sumas $(2, 4)$, $(2, 6)$ y $(2, 9)$ contenidas en $(6, 4)$.

La solución de la ecuación $X = 0$ según se desarrolla de la investigación precedente.

352.

El teorema anterior junto con sus corolarios contiene los principios básicos de la teoría completa, y el método de hallazgo de los valores de las raíces Ω puede ser tratado ahora en unas pocas palabras.

Primero hay que tomar un número g que sea una raíz primitiva para el módulo n y encontrar el residuo mínimo de las potencias de g hasta g^{n-2} según el módulo n. Resuelva $n - 1$ en factores, y de hecho en factores primos si es conveniente reducir el problema a ecuaciones del menor grado posible. Estos se llaman (el orden es arbitrario) α, β, γ, $\ldots\zeta$ y defina

$$\frac{n-1}{\alpha} = \beta\gamma\ldots\zeta = a, \qquad \frac{n-1}{\alpha\beta} = \gamma\ldots\zeta = b, \quad \text{etc.}$$

Distribuya todas la raíces Ω en α períodos de a términos, y de nuevo cada uno de éstos en β períodos de b términos, y nuevamente cada uno de éstos en γ períodos, etc.

Determine como en el artículo precedente la ecuación (A) de grado α, cuyas raíces son las α sumas de a términos; sus valores pueden ser determinados resolviendo esta ecuación.

Pero aquí surge una dificultad porque parece incierto qué sumas deben hacerse iguales a qué raíces de la ecuación (A); esto es, cuál raíz debe ser denotada por $(a,1)$, cuál por (a,g), etc. Podemos resolver esta dificultad de la siguiente forma. Designamos con $(a,1)$ una raíz cualquiera de la ecuación (A); en efecto, como cualquier raíz de esta ecuación es la suma de a raíces de Ω, y es completamente arbitrario cual raíz de Ω se denota por [1], es posible asumir que [1] expresa una de las raíces que constituyen una raíz dada de la ecuación (A), y de aquí esta raíz de la ecuación (A) será $(a,1)$. Aún así la raíz [1] no estará completamente determinada; todavía permanece completamente arbitrario o indefinido cuál de las raíces que componen $(a,1)$ escogemos para adoptar como [1]. Tan pronto como $(a,1)$ sea determinada, todas las sumas restantes de a términos pueden ser racionalmente deducidas de ella (art. 346). Así, es claro que es necesario resolver para una sola raíz de la ecuación. También se puede usar el siguiente método, menos directo, para el mismo propósito. Tome para [1] una raíz definida; i.e. sea $[1] = \cos\frac{kP}{n} + i\,\mathrm{sen}\,\frac{kP}{n}$ con el entero k tomado arbitrariamente pero de tal manera que no sea divisible por n. Cuando se hace esto, también [2], [3], etc. determinarán raíces definidas, y las sumas $(a,1)$, (a,g), etc. designarán cantidades definidas. Ahora, si estas cantidades son calculadas de una tabla de senos con precisión tal que se pueda decidir cuáles son las más grandes y cuáles las más pequeñas, ésta será dejada como la manera de distinguir sin duda las raíces individuales de la ecuación (A).

Cuando de esta forma se han encontrado todas las α sumas de a términos, determínese por los métodos del artículo precedente la ecuación (B) de grado β, cuyas raíces son las β sumas de b términos contenidas en $(a,1)$; todos los coeficientes de esta ecuación serán cantidades conocidas. Ya que en esta etapa es arbitrario cual de los $a = \beta b$ raíces contenidas en $(a,1)$ es denotada por [1], cualquier raíz dada de la ecuación (B) puede ser expresada por $(b,1)$ porque es lícito suponer que una de las b raíces de las cuales está compuesta es denotada por [1]. Determínese por lo tanto una raíz cualquiera de la ecuación (B) por una solución de ésta. Sea ella $= (b,1)$ y derive de ésta por el artículo 346 todas las restantes sumas de b términos. De esta manera tenemos al mismo tiempo un método de corroboración de los cálculos, puesto que el total de todas las sumas de b términos que pertenecen a un período cualquiera de a términos es conocido. En algunos casos es igualmente fácil formar otras $\alpha - 1$ ecuaciones de grado β, cuyas raíces sean respectivamente las β sumas individuales

de b términos contenidas en los restantes períodos de a términos (a, g), (a, g^2), etc. y determinar *todas* las raíces mediante la solución tanto de estas ecuaciones como de la ecuación B. Entonces, de la misma manera que antes, con la ayuda de una tabla de senos, podemos decidir cuáles son los períodos de b términos para los cuales las raíces individuales encontradas de esta manera son iguales. Pero para ayudar en esta decisión pueden ser usados varios otros mecanismos que no se pueden explicar plenamente aquí. Uno de ellos, sin embargo, el caso donde $\beta = 2$, es especialmente útil y puede ser explicado más brevemente por ilustración que por reglas. Lo utilizaremos en los siguientes ejemplos.

Después de encontrar los valores de todos las $\alpha\beta$ sumas de b términos de esta forma, se puede utilizar un método similar para determinar por ecuaciones de grado γ todas las $\alpha\beta\gamma$ sumas de c términos. Esto es, se puede *o* encontrar *una* ecuación de grado γ de acuerdo con el artículo 350, cuyas raíces son las γ sumas de c términos contenidos en $(b, 1)$, y resolviendo ésta encontrar una raíz que se llama $(c, 1)$ y finalmente de esto por los métodos del artículo 346 deducir todas las sumas restantes; *o* de manera similar encontrar las $\alpha\beta$ ecuaciones de grado γ cuyas raíces son respectivamente las γ sumas de c términos contenidas en los períodos individuales de b términos. Se puede resolver todas estas ecuaciones para todas sus raíces y determinar el orden de las raíces con la ayuda de una tabla de senos como hicimos antes. Sin embargo, para $\gamma = 2$ se puede usar el mecanismo que mostraremos más abajo.

Continuando de esta manera finalmente habrá todas las $\frac{n-1}{\zeta}$ sumas de ζ términos; y si se encuentra por los métodos del artículo 348 la ecuación de grado ζ cuyas raíces son las ζ raíces de Ω contenidas en $(\zeta, 1)$, todos sus coeficientes serán cantidades conocidas. Y si resolvemos para una raíz cualquiera, se puede hacerla $= [1]$, y sus potencias darán todas las otras raíces Ω. Si nos gusta más, podemos resolver para *todas* las raíces de esa ecuación. Entonces mediante la solución de las otras $\frac{n-1}{\zeta} - 1$ ecuaciones de grado ζ, las cuales contienen respectivamente todas las ζ raíces en cada uno de los restantes períodos de ζ términos, se puede encontrar todas las restantes raíces Ω.

Es claro, sin embargo, que en tanto que la primera ecuación (A) sea resuelta, o en tanto que se tengan los valores de todas las α sumas de a términos, tendremos también la resolución de X en α factores de grado a, por el artículo 348. Luego, después de resolver la ecuación (B) o después de encontrar los valores de todas las $\alpha\beta$ sumas de b términos, cada uno de esos factores será resuelto asimismo en β factores, y así X será resuelto en $\alpha\beta$ factores de grado b, etc.

Ejemplo para $n = 19$ donde la operación se reduce a resolver dos ecuaciones cúbicas y una cuadrática.

353.

Primer ejemplo para $n = 19$. Ya que aquí $n - 1 = 3 \cdot 3 \cdot 2$, la búsqueda de las raíces Ω se reduce a la solución de dos ecuaciones cúbicas y una cuadrática. Este ejemplo es entendido más fácilmente porque para la mayor parte las operaciones necesarias ya han sido discutidas antes. Tomando el número 2 como la raíz primitiva g, los residuos mínimos de sus potencias producirán lo siguiente (los exponentes de las potencias están escritos en la primera línea y los residuos en la segunda):

$$\begin{array}{c} 0.\ 1.\ 2.\ 3.\ \ 4.\ \ 5.\ 6.\ \ 7.\ 8.\ \ 9.\ 10.\ 11.\ 12.\ 13.\ 14.\ 15.\ 16.\ 17 \\ 1.\ 2.\ 4.\ 8.\ 16.\ 13.\ 7.\ 14.\ 9.\ 18.\ 17.\ 15.\ 11.\ \ 3.\ \ 6.\ 12.\ \ 5.\ 10 \end{array}$$

De esto, por los artículos 344 y 345, se deduce fácilmente la siguiente distribución de todas las raíces Ω en tres períodos de seis términos y de cada uno de ellos en tres períodos de dos términos:

$$\Omega = \quad (18,1) \left\{ \begin{array}{lll} (6,1) \left\{ \begin{array}{lll} (2,\ 1) & \ldots & [1],\ [18] \\ (2,\ 8) & \ldots & [8],\ [11] \\ (2,\ 7) & \ldots & [7],\ [12] \end{array} \right. \\ (6,2) \left\{ \begin{array}{lll} (2,\ 2) & \ldots & [2],\ [17] \\ (2{,}16) & \ldots & [3],\ [16] \\ (2{,}14) & \ldots & [5],\ [14] \end{array} \right. \\ (6,4) \left\{ \begin{array}{lll} (2,\ 4) & \ldots & [4],\ [15] \\ (2{,}13) & \ldots & [6],\ [13] \\ (2,\ 9) & \ldots & [9],\ [10] \end{array} \right. \end{array} \right.$$

La ecuación (A), cuyas raíces son las sumas $(6,1)$, $(6,2)$ y $(6,4)$, resulta ser $x^3 + x^2 - 6x - 7 = 0$ y una de las raíces es $-1{,}2218761623$. Expresando en términos de $(6,1)$, tenemos

$$(6,2) = 4 - (6,1)^2 = 2{,}5070186441$$
$$(6,4) = -5 - (6,1) + (6,1)^2 = -2{,}2851424818$$

Así X se resuelve en tres factores de grado 6, si estos valores son sustituidos en las fórmulas del artículo 348.

La ecuación (B), cuyas raíces son las sumas $(2,1)$, $(2,7)$ y $(2,8)$, resulta ser

$$x^3 - (6,1)x^2 + [(6,1) + (6,4)]x - 2 - (6,2) = 0$$

o

$$x^3 + 1{,}2218761623x^2 - 3{,}5070186441x - 4{,}5070186441 = 0$$

Una raíz es $-1{,}3545631433$ que llamaremos $(2,1)$. Por el método del artículo 346 se encuentran las siguientes ecuaciones donde, por brevedad, se escribe q en vez de $(2,1)$:

$$\begin{aligned}
(2,2) &= q^2 - 2 \\
(2,3) &= q^3 - 3q \\
(2,4) &= q^4 - 4q^2 + 2 \\
(2,5) &= q^5 - 5q^3 + 5q \\
(2,6) &= q^6 - 6q^4 + 9q^2 - 2 \\
(2,7) &= q^7 - 7q^5 + 14q^3 - 7q \\
(2,8) &= q^8 - 8q^6 + 20q^4 - 16q^2 + 2 \\
(2,9) &= q^9 - 9q^7 + 27q^5 - 30q^3 + 9q
\end{aligned}$$

En el presente caso estas ecuaciones pueden ser encontradas más fácilmente del modo siguiente que por los métodos del artículo 346. Suponiendo

$$[1] = \cos\frac{kP}{19} + i\,\mathrm{sen}\,\frac{kP}{19}$$

tenemos

$$[18] = \cos\frac{18kP}{19} + i\,\mathrm{sen}\,\frac{18kP}{19} = \cos\frac{kP}{19} - i\,\mathrm{sen}\,\frac{kP}{19}$$

y así

$$(2,1) = 2\cos\frac{kP}{19}$$

y en general

$$[\lambda] = \cos\frac{\lambda kP}{19} + i\,\mathrm{sen}\,\frac{\lambda kP}{19}, \quad \text{y así} \quad (2,\lambda) = [\lambda] + [18\lambda] = [\lambda] + [-\lambda] = 2\cos\frac{\lambda kP}{19}$$

Por lo tanto si $\frac{1}{2}q = \cos\omega$, resultará $(2,2) = 2\cos 2\omega$, $(2,3) = 2\cos 3\omega$, etc., y las mismas fórmulas de antes serán derivadas del conocimiento de ecuaciones para los

cosenos de ángulos múltiples. Ahora, de estas fórmulas se derivan los siguientes valores numéricos:

$$\begin{array}{l|l} (2,2) = -0{,}1651586909 & (2,6) = \quad 0{,}4909709743 \\ (2,3) = \quad 1{,}5782810188 & (2,7) = -1{,}7589475024 \\ (2,4) = -1{,}9727226068 & (2,8) = \quad 1{,}8916344834 \\ (2,5) = \quad 1{,}0938963162 & (2,9) = -0{,}8033908493 \end{array}$$

Los valores de $(2,7)$ y $(2,8)$ pueden encontrarse de la ecuación (B) donde son las dos raíces restantes. La duda sobre *cual* de estas raíces es $(2,7)$ y cual es $(2,8)$ puede eliminarse por un cálculo aproximado de acuerdo con las fórmulas dadas antes o por medio de tablas de senos. Una rápida consulta nos muestra que $(2,1) = 2\cos\omega$ haciendo $\omega = \frac{7}{19}P$ y así tenemos

$$(2,7) = 2\cos\frac{49}{19}P = 2\cos\frac{8}{19}P, \quad \text{y} \quad (2,8) = 2\cos\frac{56}{19}P = 2\cos\frac{1}{19}P$$

Similarmente podemos encontrar las sumas $(2,2)$, $(2,3)$ y $(2,5)$ también por la ecuación

$$x^3 - (6,2)x^2 + [(6,1) + (6,2)]x - 2 - (6,4) = 0$$

cuyas raíces son ellas, y la incertidumbre sobre qué raíces corresponden a qué sumas se puede eliminar exactamente de la misma manera que antes. Finalmente, las sumas $(2,4)$, $(2,6)$ y $(2,9)$ se pueden encontrar por la ecuación

$$x^3 - (6,4)x^2 + [(6,2) + (6,4)]x - 2 - (6,1) = 0$$

[1] y [18] son las raíces de la ecuación $x^2 - (2,1)x + 1 = 0$. Una de ellas será

$$= \frac{1}{2}(2,1) - i\sqrt{1 - \frac{1}{4}(2,1)^2} = \frac{1}{2}(2,1) + i\sqrt{\frac{1}{2} - \frac{1}{4}(2,2)}$$

y la otra

$$= \frac{1}{2}(2,1) - i\sqrt{\frac{1}{2} - \frac{1}{4}(2,2)}$$

y los valores numéricos serán $= -0{,}6772815716 \pm 0{,}7357239107\,i$. Las dieciseis raíces restantes pueden ser encontradas de las potencias de una u otra de estas raíces o resolviendo las otras ocho ecuaciones similares. Para decidir, en el segundo método

cual raíz tiene el signo positivo para su parte imaginaria y cual el negativo, podemos usar tablas de senos o el artificio que explicamos en el siguiente ejemplo. De esta manera encontraremos los siguientes valores, con el signo superior correspondiendo a la primera raíz y el signo inferior a la segunda raíz:

$$\begin{aligned}
[1] \text{ y } [18] &= -0{,}6772815716 \pm 0{,}7357239107\, i \\
[2] \text{ y } [17] &= -0{,}0825793455 \mp 0{,}9965844930\, i \\
[3] \text{ y } [16] &= 0{,}7891405094 \pm 0{,}6142127127\, i \\
[4] \text{ y } [15] &= -0{,}9863613034 \pm 0{,}1645945903\, i \\
[5] \text{ y } [14] &= 0{,}5469481581 \mp 0{,}8371664783\, i \\
[6] \text{ y } [13] &= 0{,}2454854871 \pm 0{,}9694002659\, i \\
[7] \text{ y } [12] &= -0{,}8794737512 \mp 0{,}4759473930\, i \\
[8] \text{ y } [11] &= 0{,}9458172417 \mp 0{,}3246994692\, i \\
[9] \text{ y } [10] &= -0{,}4016954247 \pm 0{,}9157733267\, i
\end{aligned}$$

Ejemplo para $n = 17$ donde la operación se reduce a resolver cuatro ecuaciones cuadráticas.

354.

Segundo ejemplo para $n = 17$. Aquí $n-1 = 2\cdot 2\cdot 2\cdot 2$, así el cálculo se reducirá a cuatro ecuaciones cuadráticas. Para la raíz primitiva tomaremos el número 3, cuyas potencias tienen residuos mínimos según el módulo 17 que son

0.	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15
1.	3.	9.	10.	13.	5.	15.	11.	16.	14.	8.	7.	4.	12.	2.	6

De esto derivamos la siguiente distribución del conjunto Ω en dos períodos de ocho términos, cuatro de cuatro términos, ocho de dos términos:

$$\Omega = (16,1)\left\{\begin{array}{ll}
(8,1)\left\{\begin{array}{ll}
(4,\ 1)\left\{\begin{array}{lll} (2,\ 1) & \ldots & [1],\ [16] \\ (2{,}13) & \ldots & [4],\ [13] \end{array}\right. \\
(4,\ 9)\left\{\begin{array}{lll} (2,\ 9) & \ldots & [8],\ [9] \\ (2{,}15) & \ldots & [2],\ [15] \end{array}\right.
\end{array}\right. \\
(8,3)\left\{\begin{array}{ll}
(4,\ 3)\left\{\begin{array}{lll} (2,\ 3) & \ldots & [3],\ [14] \\ (2,\ 5) & \ldots & [5],\ [12] \end{array}\right. \\
(4,10)\left\{\begin{array}{lll} (2{,}10) & \ldots & [7],\ [10] \\ (2{,}11) & \ldots & [6],\ [11] \end{array}\right.
\end{array}\right.
\end{array}\right.$$

Se encuentra por las reglas del artículo 351 que la ecuación (A), cuyas raíces son las sumas $(8,1)$ y $(8,3)$, es $x^2 + x - 4 = 0$. Sus raíces son $-\frac{1}{2} + \frac{1}{2}\sqrt{17} = 1{,}5615528128$ y $-\frac{1}{2} - \frac{1}{2}\sqrt{17} = -2{,}5615528128$. Haremos la primera $= (8,1)$ y así necesariamente la última $= (8,3)$.

La ecuación (B), cuyas raíces son las sumas $(4,1)$ y $(4,9)$, es $x^2 - (8,1)x - 1 = 0$. Sus raíces son $\frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{4 + (8,1)^2} = \frac{1}{2}(8,1) \pm \frac{1}{2}\sqrt{12 + 3(8,1) + 4(8,3)}$. Haremos $(4,1)$ igual a la cantidad que tenga el signo radical positivo y cuyo valor numérico es $2{,}0494811777$. Así la cantidad con el signo del radical negativo y cuyo valor numérico es $-0{,}4879283649$ será expresada por $(4,9)$. Las sumas restantes de cuatro términos, a saber $(4,3)$ y $(4,10)$, pueden ser calculadas de dos maneras. *Primera,* por el método del artículo 346, que da las siguientes fórmulas cuando abreviamos $(4,1)$ con la letra p:

$$(4,3) = -\frac{3}{2} + 3p - \frac{1}{2}p^3 = 0{,}3441507314$$
$$(4,10) = \frac{3}{2} + 2p - p^2 - \frac{1}{2}p^3 = -2{,}9057035442$$

El mismo método da la fórmula $(4,9) = -1 - 6p + p^2 + p^3$ y de ésta obtenemos el mismo valor que antes. El *segundo* método permite determinar las sumas $(4,3)$ y $(4,10)$ resolviendo la ecuación $x^2 - (8,3)x - 1 = 0$ de la que ellas son las raíces. Estas raíces son $\frac{1}{2}(8,3) \pm \frac{1}{2}\sqrt{4 + (8,3)^2}$, o sea

$$\frac{1}{2}(8,3) + \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)} \quad \text{y} \quad \frac{1}{2}(8,3) - \frac{1}{2}\sqrt{12 + 4(8,1) + 3(8,3)}$$

Se puede remover la duda de *cual* raíz debe ser expresada por $(4,3)$ y cual por $(4,10)$ mediante el siguiente artificio que mencionamos en el artículo 352. Calcule el producto de $(4,1) - (4,9)$ por $(4,3) - (4,10)$ que es $= 2(8,1) - 2(8,3)$ *). Ahora el valor de esta expresión es positivo $= +2\sqrt{17}$ y, ya que el primer factor del producto, $(4,1) - (4,9) = +\sqrt{12 + 3(8,1) + 4(8,3)}$, es positivo, el otro factor $(4,3) - (4,10)$, deberá ser también positivo. Por lo tanto $(4,3)$ es igual a la primera raíz que tiene el signo positivo enfrente del radical, y $(4,10)$ es igual a la segunda raíz. De esto resultarán los mismos valores numéricos que antes.

Habiendo encontrado todas las sumas de cuatro términos, procedemos a las sumas de dos términos. La ecuación (C), cuyas raíces son $(2,1)$ y $(2,13)$ y está

*) La base real de este artificio es el hecho, fácil de prever, que el producto no contiene sumas de cuatro términos sino únicamente sumas de ocho términos. El matemático entrenado puede comprender fácilmente la razón de esto. Por brevedad la omitiremos aquí.

contenida en $(4,1)$, será $x^2 - (4,1)x + (4,3) = 0$. Sus raíces son

$$\frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{-4(4,3) + (4,1)^2} \quad \text{o sea} \quad \frac{1}{2}(4,1) \pm \frac{1}{2}\sqrt{4 + (4,9) - 2(4,3)}$$

Cuando tomamos la cantidad radical positiva, obtenemos el valor 1,8649444588, la que hacemos $= (2,1)$ y así $(2,13)$ será igual a la otra cuyo valor es $= 0{,}1845367189$. Si las sumas restantes de dos términos han de ser encontradas por el método del artículo 346, se pueden usar las mismas fórmulas para $(2,2)$, $(2,3)$, $(2,4)$, $(2,5)$, $(2,6)$, $(2,7)$ y $(2,8)$ como lo hicimos en el ejemplo precedente para cantidades similares, es decir, $(2,2)$ (o $(2,15)$) $= (2,1)^2 - 2$ etc. Pero si parece preferible encontrarlas en pares resolviendo una ecuación cuadrática, para $(2,9)$ y $(2,15)$ obtenemos la ecuación $x^2 - (4,9)x + (4,10) = 0$ cuyas raíces son $\frac{1}{2}(4,9) \pm \frac{1}{2}\sqrt{4 + (4,1) - 2(4,10)}$. Se puede determinar que signo usar del mismo modo que antes. Calculando el producto de $(2,1) - (2,13)$ por $(2,9) - (2,15)$ resulta $-(4,1) + (4,9) - (4,3) + (4,10)$. Ya que éste es negativo y el factor $(2,1) - (2,13)$ es positivo, $(2,9) - (2,15)$ deberá ser negativo y es necesario usar el signo superior positivo para $(2,15)$ y el signo inferior negativo para $(2,9)$. De esto se computa que $(2,9) = -1{,}9659461994$ y $(2,15) = 1{,}4780178344$. Entonces, ya que calculando el producto de $(2,1) - (2,13)$ por $(2,3) - (2,5)$ resulta la cantidad positiva $(4,9) - (4,10)$, el factor $(2,3) - (2,5)$ debe ser positivo. Y por un cálculo parecido al anterior se encuentra

$$(2,3) = \frac{1}{2}(4,3) + \frac{1}{2}\sqrt{4 + (4,10) - 2(4,9)} = \quad 0{,}8914767116$$
$$(2,5) = \frac{1}{2}(4,3) - \frac{1}{2}\sqrt{4 + (4,10) - 2(4,9)} = -0{,}5473259801$$

Finalmente, mediante operaciones completamente análogas se descubre

$$(2,10) = \frac{1}{2}(4,10) - \frac{1}{2}\sqrt{4 + (4,3) - 2(4,1)} = -1{,}7004342715$$
$$(2,11) = \frac{1}{2}(4,10) + \frac{1}{2}\sqrt{4 + (4,3) - 2(4,1)} = -1{,}2052692728$$

Resta ahora descender a las raíces Ω mismas. La ecuación (D) cuyas raíces son $[1]$ y $[16]$ nos da $x^2 - (2,1)x + 1 = 0$. Las raíces de ella son $\frac{1}{2}(2,1) \pm \frac{1}{2}\sqrt{(2,1)^2 - 4}$ o mejor dicho

$$\frac{1}{2}(2,1) \pm \frac{1}{2}i\sqrt{4 - (2,1)^2} \quad \text{o sea} \quad \frac{1}{2}(2,1) \pm \frac{1}{2}i\sqrt{2 - (2,15)}$$

Tomaremos los signos superiores para [1], los inferiores para [16]. Se deducen las catorce raíces restantes de las potencias de [1] o por la solución de siete ecuaciones cuadráticas, cada una de las cuales nos dará dos raíces, y la incertidumbre acerca de los signos de las cantidades radicales puede ser removida mediante el mismo mecanismo usado antes. Así [4] y [13] son las raíces de la ecuación $x^2-(2,13)x+1=0$ y así igual a $\frac{1}{2}(2,13) \pm \frac{1}{2}i\sqrt{2-(2,9)}$. Calculando el producto de $[1]-[16]$ por $[4]-[13]$ sin embargo obtenemos $(2,5)-(2,3)$, una cantidad real negativa. Por lo tanto, puesto que $[1]-[16]$ es $+i\sqrt{2-(2,15)}$, i.e. el producto imaginario i por una cantidad real *positiva,* $[4]-[13]$ debe también ser el producto de i por una cantidad real *positiva*, porque $i^2 = -1$. Como conclusión tomaremos el signo superior para [4] y el signo inferior para [13]. Similarmente para las raíces [8] y [9] encontramos $\frac{1}{2}(2,9) \pm \frac{1}{2}i\sqrt{2-(2,1)}$ así, ya que el producto de $[1]-[16]$ por $[8]-[9]$ es $(2,9)-(2,10)$ y negativo, debemos tomar el signo superior para [8] y el signo inferior para [9]. Si computamos entonces las restantes raíces obtendremos los siguientes valores numéricos, donde el signo superior ha de ser tomado para la primera raíz y el signo inferior para la segunda:

$$
\begin{aligned}
[1],[16]\ldots &\quad 0{,}9324722294 \pm 0{,}3612416662\,i \\
[2],[15]\ldots &\quad 0{,}7390089172 \pm 0{,}6736956436\,i \\
[3],[14]\ldots &\quad 0{,}4457383558 \pm 0{,}8951632914\,i \\
[4],[13]\ldots &\quad 0{,}0922683595 \pm 0{,}9957341763\,i \\
[5],[12]\ldots &-0{,}2736629901 \pm 0{,}9618256432\,i \\
[6],[11]\ldots &-0{,}6026346364 \pm 0{,}7980172273\,i \\
[7],[10]\ldots &-0{,}8502171357 \pm 0{,}5264321629\,i \\
[8],[\ 9]\ldots &-0{,}9829730997 \pm 0{,}1837495178\,i
\end{aligned}
$$

Lo que precede puede bastar para resolver la ecuación $x^n - 1 = 0$ y así también para encontrar las funciones trigonométricas correspondientes a los arcos que son conmesurables con la circunferencia. Pero esta materia es tan importante que no podemos concluir sin indicar algunas de las observaciones que arrojan luz sobre el tema, lo mismo que ejemplos relacionados con él o que dependen de él. Entre éstos seleccionaremos específicamente aquéllos que pueden ser resueltos sin una gran cantidad de aparato que depende de otras investigaciones y los consideramos solamente como *ejemplos* de esta inmensa teoría que deberá ser considerada detalladamente en una ocasión posterior.

Investigaciones adicionales sobre los períodos de raíces.
Sumas con un número par de términos son cantidades reales.

355.

Ya que siempre n se supone impar, 2 estará entre los factores de $n-1$, y el conjunto Ω estará compuesto de $\frac{1}{2}(n-1)$ períodos de dos términos. Un tal período $(2,\lambda)$ consistirá de las raíces $[\lambda]$ y $[\lambda g^{\frac{1}{2}(n-1)}]$, denotando, como antes, g como cualquier raíz primitiva para el módulo n. Pero $g^{\frac{1}{2}(n-1)} \equiv -1 \pmod{n}$ y así $\lambda g^{\frac{1}{2}(n-1)} \equiv -\lambda$ (ver art. 62) y $[\lambda g^{\frac{1}{2}(n-1)}] = [-\lambda]$. Por lo tanto, suponiendo que $[\lambda] = \cos\frac{kP}{n} + i\,\mathrm{sen}\,\frac{hP}{n}$ y $[-\lambda] = \cos\frac{kP}{n} - i\,\mathrm{sen}\,\frac{kP}{n}$, resulta la suma $(2,\lambda) = 2\cos\frac{kP}{n}$. Hasta este punto únicamente deducimos la conclusión de que el valor de cualquier suma de dos términos es una cantidad real. Puesto que cualquier período que tenga un número par de términos $= 2a$ se puede descomponer en a períodos de dos términos, en general es claro que el valor de cualquier suma que tenga un número par de términos es siempre una cantidad real. Por lo tanto, si en el artículo 352 entre los factores α, β, γ, etc., se reservan dos hasta el final, todas las operaciones serán hechas sobre cantidades reales hasta que lleguemos a una suma de dos términos, y los imaginarios serán introducidos cuando pasamos de estas sumas a las raíces mismas.

De la ecuación que define la distribución de las raíces Ω en dos períodos.

356.

Merecen atención especial las ecuaciones auxiliares mediante las cuales se determinan para cualquier valor de n las sumas que forman el conjunto Ω. Ellas están conectadas de una manera sorprendente con las propiedades más recónditas del número n. Aquí nos restringiremos al estudio de los dos casos siguientes. *Primero,* la ecuación cuadrática cuyas raíces son sumas de $\frac{1}{2}(n-1)$ términos, *segundo,* en caso de que $n-1$ tenga el factor 3, consideraremos la ecuación cúbica cuyas raíces son sumas de $\frac{1}{3}(n-1)$ términos.

Escribiendo por brevedad m en lugar de $\frac{1}{2}(n-1)$ y designando por g alguna raíz primitiva para el módulo n, el conjunto Ω consistirá de dos períodos $(m,1)$ y (m,g). El primero contendrá las raíces $[1]$, $[g^2]$, $[g^4]$, $\ldots$ $[g^{n-3}]$, el último las raíces $[g]$, $[g^3]$, $[g^5]$, $\ldots$ $[g^{n-2}]$. Suponiendo que los residuos mínimos positivos de los números g^2, g^4,$\ldots$ g^{n-3} según el módulo n son, en orden arbitrario, R, R', R'', etc. y los residuos de g, g^3, g^5, $\ldots$ g^{n-2} son N, N', N'', etc., entonces las raíces de las que consiste $(m,1)$, coinciden con $[1]$, $[R]$, $[R']$, $[R'']$, etc. y las raíces del período (m,g) con $[N]$, $[N']$, $[N'']$, etc. Es claro que todos los números 1, R, R', R'', etc. son *residuos*

cuadráticos del número n. Puesto que todos ellos son diferentes y menores que n, y ya que su número es $= \frac{1}{2}(n-1)$ y así igual al número de todos los residuos positivos de n que son menores que n, estos residuos coincidirán completamente con aquellos números. Igualmente, todos los números N, N', N'', etc. son diferentes uno del otro y de los números 1, R, R', etc. y junto con éstos agotan todos los números 1, 2, 3, $\ldots n-1$. Se sigue que los números N, N', N'', etc. deben coincidir con todos los *no residuos cuadráticos* positivos de n que son menores que n. Ahora, si se supone que la ecuación cuyas raíces son las sumas $(m,1)$ y (m,g) es

$$x^2 - Ax + B = 0$$

resulta

$$A = (m,1) + (m,g) = -1, \qquad B = (m,1) \cdot (m,g)$$

El producto de $(m,1)$ por (m,g) es, por el artículo 345,

$$= (m, N+1) + (m, N'+1) + (m, N''+1) + \text{ etc.} = W$$

y de ese modo se reducirá a una forma $\alpha(m,0) + \beta(m,1) + \gamma(m,g)$. Para determinar los coeficientes α, β y γ observamos *primero* que $\alpha+\beta+\gamma = m$ (porque el número de sumas en $W = m$); *segundo,* que $\beta = \gamma$ (esto sigue del artículo 350 pues el producto $(m,1) \cdot (m,g)$ es una función invariable de las sumas $(m,1)$ y (m,g) de las que se compone la suma más grande $(n-1,1)$); *tercero,* puesto que todos los números $N+1$, $N'+1$, $N''+1$, etc. están contenidos entre las cotas 2 y $n+1$, es claro que *o* ninguna suma en W puede ser reducida a $(m,0)$ y así $\alpha = 0$ cuando el número $n-1$ no se halla entre los números N, N', N'', etc. *o* que una suma, digamos (m,n) puede ser reducida a $(m,0)$ y así $\alpha = 1$ cuando $n-1$ no se halla entre los números N, N', N'', etc. En el primer caso por lo tanto se infiere $\alpha = 0$, $\beta = \gamma = \frac{1}{2}m$, en el último $\alpha = 1$, $\beta = \gamma = \frac{1}{2}(m-1)$. Ya que los números β y γ deben ser enteros, se sigue que se tendrá el primer caso, esto es, $n-1$ (o lo que es lo mismo, -1) no se encontrará entre los no residuos de n cuando m es par o n es de la forma $4k+1$. El último caso se tendrá, esto es, $n-1$ o sea -1 será un no residuo de n, siempre que m sea impar o n sea de la forma $4k+3$ *). Ahora, ya que $(m,0) = m$, $(m,1) + (m,g) = -1$, el

*) De esta forma damos una nueva demostración del teorema que dice que -1 es un residuo de todos los números primos de la forma $4k+1$ y un no residuo de todos los de la forma $4k+3$. Antes (art. 108, 109 y 262) probamos esto de varias maneras diferentes. Si es preferible asumir este teorema, no habrá necesidad de distinguir entre los dos casos porque β y γ ya serán enteros.

producto buscado será $= -\frac{1}{2}m$ en el primer caso y será $= \frac{1}{2}(m+1)$ en el último. Así la ecuación en el primer caso será $x^2 + x - \frac{1}{4}(n-1) = 0$ con raíces $-\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$, en el último $x^2 + x + \frac{1}{4}(n+1)$ con raíces $-\frac{1}{2} \pm \frac{1}{2}i\sqrt{n}$.

Sea $\mathfrak{R}$ el conjunto de todos los residuos cuadráticos positivos de n que son menores que n y sea $\mathfrak{N}$ el conjunto de todos los no residuos correspondientes. Entonces, no importa cuál raíz de Ω sea escogida por [1], la diferencia entre las sumas $\sum[\mathfrak{R}]$ y $\sum[\mathfrak{N}]$ será $= \pm\sqrt{n}$ para $n \equiv 1$ e $= \pm i\sqrt{n}$ para $n \equiv 3 \pmod 4$. Se sigue que si k es cualquier entero no divisible por n

$$\sum \cos\frac{k\mathfrak{R}P}{n} - \sum \cos\frac{k\mathfrak{N}P}{n} = \pm\sqrt{n} \quad \text{y} \quad \sum \operatorname{sen}\frac{k\mathfrak{R}P}{n} - \sum \operatorname{sen}\frac{k\mathfrak{N}P}{n} = 0$$

para $n \equiv 1 \pmod 4$. Por otra parte para $n \equiv 3 \pmod 4$ la primera diferencia será $= 0$ y la segunda $= \pm\sqrt{n}$. Estos teoremas son tan elegantes que merecen una distinción especial. Observamos que los signos superiores siempre se mantienen cuando en vez de k se toma la unidad o un residuo cuadrático de n y los inferiores cuando k es un no residuo. Estos teoremas mantienen la misma o aún mayor elegancia cuando son extendidos a valores compuestos de n. Pero estas materias están en un nivel superior de investigación y reservaremos sus consideraciones para otra ocasión.

Demostración de un teorema mencionado en Sección IV.

357.

Sea

$$z = x^m - ax^{m-1} + bx^{m-2} - \text{ etc.} = 0$$

la ecuación de grado m cuyas raíces son las m raíces contenidas en el período $(m, 1)$. Aquí $a = (m, 1)$ y cada uno de los coeficientes restantes b, etc. serán de la forma $\mathfrak{A} + \mathfrak{B}(m, 1) + \mathfrak{C}(m, g)$ con $\mathfrak{A}$, $\mathfrak{B}$ y $\mathfrak{C}$, enteros (art.348). Denotando por z' la función en la que se transforma z cuando se sustituyen $(m, 1)$ por (m, g) en todas partes y (m, g) por (m, g^2), o lo que es la misma cosa $(m, 1)$, entonces las raíces de la ecuación $z' = 0$ serán las raíces contenidas en (m, g) y el producto

$$zz' = \frac{x^n - 1}{x - 1} = X$$

Por lo tanto z puede ser reducida a la forma $R + S(m, 1) + T(m, g)$ donde R, S y T serán funciones enteras de x con todos sus coeficientes enteros. Hecho esto, resulta

$$z' = R + S(m, g) + T(m, 1)$$

Y si por brevedad escribimos p y q por $(m,1)$ y (m,g) respectivamente

$$2z = 2R + (S+T)(p+q) - (T-S)(p-q) = 2R - S - T - (T-S)(p-q)$$

y similarmente

$$2z' = 2R - S - T + (T-S)(p-q)$$

así, poniendo

$$2R - S - T = Y, \qquad T - S = Z$$

resulta $4X = Y^2 - (p-q)^2 Z^2$ y ya que $(p-q)^2 = \pm n$

$$4X = Y^2 \mp nZ^2$$

El signo superior vale cuando n es de la forma $4k+1$, el inferior cuando n es de la forma $4k+3$. Este es el teorema que prometimos probar (art. 124). Es fácil ver que los dos términos de mayor grado en la función Y siempre serán $2x^m + x^{m-1}$ y el mayor en la función Z, x^{m-1}. Todos los coeficientes restantes serán enteros, variarán de acuerdo con la naturaleza del número n y no se puede dar una fórmula analítica general.

Ejemplo. Para $n = 17$, por las reglas del artículo 348, la ecuación cuyas raíces son las ocho raíces contenidas en (8,1) será

$$x^8 - px^7 + (4+p+2q)x^6 - (4p+3q)x^5 + (6+3p+5q)x^4 \\ -(4p+3q)x^3 + (4+p+2q)x^2 - px + 1 = 0$$

por lo tanto

$$R = x^8 + 4x^6 + 6x^4 + 4x^2 + 1$$
$$S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + x^2 - x$$
$$T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2x^2$$

y

$$Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5x^2 + x + 2$$
$$Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + x^2 + x$$

He aquí algunos otros ejemplos

n	Y	Z
3	$2x+1$	1
5	$2x^2+x+2$	x
7	$2x^3+x^2-x-2$	x^2+x
11	$2x^5+x^4-2x^3+2x^2-x-2$	x^4+x
13	$2x^6+x^5+4x^4-x^3+4x^2+x+2$	x^5+x^3+x
19	$2x^9+x^8-4x^7+3x^6+5x^5-5x^4$ $-3x^3+4x^2-x-2$	$x^8-x^6+x^5+x^4-x^3+x$
23	$2x^{11}+x^{10}-5x^9-8x^8-7x^7-4x^6$ $+4x^5+7x^4+8x^3+5x^2-x-2$	$x^{10}+x^9-x^7-2x^6-2x^5$ $-x^4+x^2+x$

De la ecuación que distribuye las raíces Ω en tres períodos.

358.

Procedemos ahora a la consideración de las ecuaciones cúbicas que determinan las tres sumas de $\frac{1}{3}(n-1)$ términos que componen el conjunto Ω, para el caso en que n es de la forma $3k+1$. Sea g cualquier raíz primitiva para el módulo n y $\frac{1}{3}(n-1)=m$ que será un entero par. Entonces las tres sumas que componen Ω serán $(m,1)$, (m,g) y (m,g^2), por las cuales escribimos p, p' y p'' respectivamente. Es claro que la primera contiene las raíces $[1]$, $[g^3]$, $[g^6]$, $\ldots [g^{n-4}]$, la segunda las raíces $[g]$, $[g^4]$, $\ldots [g^{n-3}]$, y la tercera las raíces $[g^2]$, $[g^5]$, $\ldots [g^{n-2}]$. Suponiendo que la ecuación buscada es

$$x^3 - Ax^2 + Bx - C = 0$$

resulta

$$A = p+p'+p'', \quad B = pp'+p'p''+pp'', \quad C = pp'p''$$

y directamente $A=-1$. Sean $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, etc., los residuos positivos mínimos de los números g^3, g^6, $\ldots g^{n-4}$ según el módulo n, en orden arbitrario, y sea $\mathfrak{K}$ el conjunto de ellos y el número 1. Similarmente sean $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, etc. los residuos mínimos de los números g, g^4, g^7, $\ldots g^{n-3}$ y $\mathfrak{K}'$ su conjunto; finalmente sean $\mathfrak{A}''$, $\mathfrak{B}''$, $\mathfrak{C}''$, etc. los residuos mínimos de g^2, g^5, g^8, $\ldots g^{n-2}$ y $\mathfrak{K}''$ su conjunto. Así todos los números en $\mathfrak{K}$, $\mathfrak{K}'$, $\mathfrak{K}''$ serán diferentes y coincidirán con 1, 2, 3, $\ldots n-1$. Primero que todo, debemos observar aquí que el número $n-1$ debe estar en $\mathfrak{K}$, pues es fácil ver que es un residuo de $g^{\frac{3m}{2}}$. También sigue de esto que los dos números h, $n-h$ se encontrarán siempre en uno *mismo* de los tres conjuntos $\mathfrak{K}$, $\mathfrak{K}'$ y $\mathfrak{K}''$, porque si

uno de ellos es un residuo de la potencia g^λ, el otro será un residuo de la potencia $g^{\lambda+\frac{3m}{2}}$ o de $g^{\lambda-\frac{3m}{2}}$ si $\lambda > \frac{3m}{2}$. Denotaremos por $(\mathfrak{RR})$ el número de enteros en la serie 1, 2, 3, $\ldots n-1$ que pertenencen a $\mathfrak{R}$ por sí mismos y cuando son aumentados en una unidad; similarmente $(\mathfrak{RR}')$ será el número de enteros en la misma serie, que están ellos mismos contenidos en $\mathfrak{R}$ pero están en $\mathfrak{R}'$ cuando son aumentados en una unidad. Será inmediatamente obvio cual es el significado de las notaciones $(\mathfrak{RR}'')$, $(\mathfrak{R}'\mathfrak{R})$, $(\mathfrak{R}'\mathfrak{R}')$, $(\mathfrak{R}'\mathfrak{R}'')$, $(\mathfrak{R}''\mathfrak{R})$, $(\mathfrak{R}''\mathfrak{R}')$ y $(\mathfrak{R}''\mathfrak{R}'')$. Hecho esto, digo *primero* que $(\mathfrak{RR}') = (\mathfrak{R}'\mathfrak{R})$. En efecto, suponiendo que h, h', h'', etc. son todos los números de la serie 1, 2, 3, $\ldots n-1$ que están ellos mismos en $\mathfrak{R}$ pero con los próximos números mayores $h+1$, $h'+1$, $h''+1$, etc. en $\mathfrak{R}'$, de modo que por definición el número de ellos es $(\mathfrak{RR}')$, entonces es claro que todos los números $n-h-1$, $n-h'-1$, $n-h''-1$, etc. están contenidos en $\mathfrak{R}'$ y los próximos números mayores $n-h$, $n-h'$, etc. en $\mathfrak{R}$; y ya que existen $(\mathfrak{R}'\mathfrak{R})$ de tales números en total, de seguro no podemos tener $(\mathfrak{R}'\mathfrak{R}) < (\mathfrak{RR}')$. Se demuestra similarmente que no es posible tener $(\mathfrak{RR}') < (\mathfrak{R}'\mathfrak{R})$, así estos números son necesariamente iguales. Exactamente de la misma manera se prueba que $(\mathfrak{RR}'') = (\mathfrak{R}''\mathfrak{R})$ y $(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}')$. *Segundo,* ya que cualquier número en $\mathfrak{R}$, con excepción del más grande, $n-1$, debe ser seguido por el siguiente mayor en $\mathfrak{R}$ o en $\mathfrak{R}'$ o en $\mathfrak{R}''$, la suma $(\mathfrak{RR}) + (\mathfrak{RR}') + (\mathfrak{RR}'')$ debe ser igual al número de todos los números en $\mathfrak{R}$ disminuido en una unidad, esto es $= m-1$. Por una razón similar

$$(\mathfrak{R}'\mathfrak{R}) + (\mathfrak{R}'\mathfrak{R}') + (\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}) + (\mathfrak{R}''\mathfrak{R}') + (\mathfrak{R}''\mathfrak{R}'') = m$$

Con estos preliminares, por las reglas del artículo 345 desarrollaremos el producto pp' en $(m, \mathfrak{A}'+1) + (m, \mathfrak{B}'+1) + (m, \mathfrak{C}'+1) +$ etc. Esta expresión se reduce fácilmente a $(\mathfrak{R}'\mathfrak{R})p + (\mathfrak{R}'\mathfrak{R}')p' + (\mathfrak{R}'\mathfrak{R}'')p''$. Por el artículo 345 se obtiene de esto el producto $p'p''$ sustituyendo $(m,1)$, (m,g) y (m,g^2) por las cantidades (m,g), (m,g^2) y (m,g^3) respectivamente, i.e., p, p' y p'' por p', p'' y p respectivamente . Así tenemos $p'p'' = (\mathfrak{R}'\mathfrak{R})p' + (\mathfrak{R}'\mathfrak{R}')p'' + (\mathfrak{R}'\mathfrak{R}'')p$ y similarmente $p''p = (\mathfrak{R}'\mathfrak{R})p'' + (\mathfrak{R}'\mathfrak{R}')p + (\mathfrak{R}'\mathfrak{R}'')p'$. De esto obtenemos *primero*

$$B = m(p + p' + p'') = -m$$

y *segundo* de una manera similar a aquélla por la cual fue desarrollado pp', se reduce también pp'' a $(\mathfrak{R}''\mathfrak{R})p + (\mathfrak{R}''\mathfrak{R}')p' + (\mathfrak{R}''\mathfrak{R}'')p''$. Y ya que esta expresión debe ser idéntica a la precedente, es necesario que $(\mathfrak{R}''\mathfrak{R}) = (\mathfrak{R}'\mathfrak{R}')$ y $(\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R})$. Ahora, poniendo

$$(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}') = a$$

$$(\mathfrak{K}''\mathfrak{K}'') = (\mathfrak{K}'\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}') = b$$
$$(\mathfrak{K}'\mathfrak{K}') = (\mathfrak{K}''\mathfrak{K}) = (\mathfrak{K}\mathfrak{K}'') = c$$

resulta $m-1 = (\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}\mathfrak{K}) + b + c$. Y ya que $a+b+c = m$, $(\mathfrak{K}\mathfrak{K}) = a-1$. Así las nueve cantidades desconocidas se reducen a tres a, b y c o mejor, ya que $a+b+c = m$, a dos. Finalmente, es claro que el cuadrado p^2 se convierte en $(m, 1+1) + (m, \mathfrak{A}+1) + (m, \mathfrak{B}+1) + (m, \mathfrak{C}+1) +$ etc. Entre los términos de esta expresión tenemos (m, n) que se reduce a $(m, 0)$ o sea a m, y los restantes términos se reducen a $(\mathfrak{K}\mathfrak{K})p + (\mathfrak{K}\mathfrak{K}')p' + (\mathfrak{K}\mathfrak{K}'')p''$, así $p^2 = m + (a-1)p + bp' + cp''$.

Como un resultado de las investigaciones anteriores tenemos las siguientes reducciones:

$$\begin{aligned} p^2 &= m + (a-1)p + bp' + cp'' \\ pp' &= bp + cp' + ap'' \\ pp'' &= cp + ap' + bp'' \\ p'p'' &= ap + bp' + cp'' \end{aligned}$$

donde las tres incógnitas satisfacen la ecuación condicional

$$a+b+c = m \qquad (I)$$

y por otra parte es cierto que estos números son enteros. Como una consecuencia tenemos

$$\begin{aligned} C = p \cdot p'p'' &= ap^2 + bpp' + cpp'' \\ &= am + (a^2+b^2+c^2-a)p + (ab+bc+ac)p' + (ab+bc+ac)p'' \end{aligned}$$

Pero ya que $pp'p''$ es una función invariable de p, p' y p'', los coeficientes por los que ellos son multiplicados en la expresión precedente son necesariamente iguales (art. 350) y hay una nueva ecuación

$$a^2+b^2+c^2-a = ab+bc+ac \qquad (II)$$

y de ésta $C = am + (ab+bc+ac)(p+p'+p'')$ o (causa de (I) y por el hecho que $p+p'+p'' = -1$)

$$C = a^2 - bc \qquad (III)$$

Ahora, aún cuando C depende de tres incógnitas y existen solamente dos ecuaciones, no obstante con la ayuda de la condición de que a, b y c son enteros, ellos serán

suficientes para determinar C completamente. Para demostrar esto, expresamos la ecuación (II) como

$$12a + 12b + 12c + 4 = 36a^2 + 36b^2 + 36c^2 - 36ab - 36ac - 36bc - 24a + 12b + 12c + 4$$

Por (I), el lado izquierdo se convierte en $= 12m + 4 = 4n$. El lado derecho se reduce a

$$(6a - 3b - 3c - 2)^2 + 27(b - c)^2$$

o, escribiendo k en vez de $2a - b - c$, a $(3k-2)^2 + 27(b-c)^2$. Así el número $4n$ (i.e. el cuádruple de cualquier número primo de la forma $3m+1$) puede ser representado por la forma $x^2 + 27y^2$. Esto puede, por supuesto, deducirse sin ninguna dificultad de la teoría general de formas binarias, pero es notable que tal descomposición está ligada a los valores de a, b y c. Ahora, el número $4n$ siempre puede ser descompuesto de una única manera en la suma de un cuadrado y 27 veces otro cuadrado. Demostraremos esto como sigue *). Si se supone que

$$4n = t^2 + 27u^2 = t'^2 + 27u'^2$$

tenemos *primero*

$$(tt' - 27uu')^2 + 27(tu' + t'u)^2 = 16n^2$$

segundo

$$(tt' + 27uu')^2 + 27(tu' - t'u)^2 = 16n^2$$

tercero

$$(tu' + t'u)(tu' - t'u) = 4n(u'^2 - u^2)$$

De esta tercera ecuación se sigue que n, por ser un número primo, divide uno de los números $tu' + t'u$, $tu' - t'u$. De la primera y segunda, sin embargo, es claro que cada uno de estos números es menor que n, así al que n divide es necesariamente $= 0$. Por lo tanto $u'^2 - u^2 = 0$ y $u'^2 = u^2$ y $t'^2 = t^2$; i.e. las dos descomposiciones no son diferentes. Supongamos ahora que se conoce la descomposición de $4n$ en un cuadrado más 27 veces un cuadrado (esto se puede hacer por el método directo de la sección V o por el método indirecto de los art. 323 y 324). Si $4n = M^2 + 27N^2$, los cuadrados $(3k-2)^2$ y $(b-c)^2$ estarán determinados y tendremos dos ecuaciones

*) Esta proposición puede probarse mucho más directamente a partir de los principios de la sección V.

en lugar de la ecuación (II). Pero claramente no solo estará determinado el cuadrado $(3k-2)^2$ sino también su raíz $3k-2$. Porque debe ser $= +M$ o $= -M$, la ambigüedad es fácilmente eliminada, pues ya que k debe ser un entero, resulta $3k-2 = +M$ o $= -M$ de acuerdo con que M sea de la forma $3z+1$ o $3z+2$ *). Ahora, puesto que $k = 2a-b-c = 3a-m$, resulta $a = \frac{1}{3}(m+k)$, $b+c = m-a = \frac{1}{3}(2m-k)$ y así

$$\begin{aligned} C = a^2 - bc &= a^2 - \frac{1}{4}(b+c)^2 + \frac{1}{4}(b-c)^2 \\ &= \frac{1}{9}(m+k)^2 - \frac{1}{36}(2m-k)^2 + \frac{1}{4}N^2 = \frac{1}{12}k^2 + \frac{1}{3}km + \frac{1}{4}N^2 \end{aligned}$$

y entonces se han encontrado todos los coeficientes de la ecuación. *Q. E. F.* Esta fórmula será mucho más simple si sustituimos N^2 por sus valores de la ecuación $(3k-2)^2 + 27N^2 = 4n = 12m+4$. Después del cálculo obtenemos

$$C = \frac{1}{9}(m+k+3km) = \frac{1}{9}(m+kn)$$

El mismo valor puede ser reducido a $(3k-2)N^2 + k^3 - 2k^2 + k - km + m$. Aunque esta expresión es menos útil, muestra inmediatamente que C resulta ser un entero, como debería.

Ejemplo. Para $n = 19$ tenemos $4n = 49 + 27$, así $3k-2 = +7$, $k = 3$, $C = \frac{1}{9}(6+57) = 7$ y la ecuación buscada es $x^3 + x^2 - 6x - 7 = 0$, como antes (art. 351). Similarmente, para $n = 7$, 13, 31, 37, 43, 61 y 67 el valor de k es respectivamente 1, -1, 2, -3, -2, 1, -1 y $C = 1$, -1, 8, -11, -8, 9, -5.

Aunque el problema que hemos resuelto en este artículo es bastante intrincado, no hemos querido omitirlo a causa de la elegancia de la solución y porque da ocasión para usar varios artificios que son fructíferos también en otras discusiones †).

---

*) Evidentemente M no puede ser de la forma $3z$ por que, de lo contrario, sería divisible por 3. Con respecto a la ambigüedad de si $b-c$ debe ser $= N$ o $= -N$, es innecesario considerar la cuestión aquí, y por la naturaleza del caso no se puede determinar porque depende de la elección de la raíz primitiva g. Para algunas raíces primitivas la diferencia $b-c$ será positiva y para otras será negativa.

†) Corolario. Sea ε una raíz de la ecuación $x^3 - 1 = 0$. Tendremos $(p + \varepsilon p' + \varepsilon^2 p'')^3 = \frac{n}{2}(M + N\sqrt{-27})$. Sean $\frac{M}{\sqrt{4n}} = \cos\varphi$ y $\frac{N\sqrt{27}}{\sqrt{4n}} = \operatorname{sen}\varphi$ y como resultado

$$p = -\frac{1}{3} + \frac{2}{3}\cos\frac{1}{3}\varphi\sqrt{n} \quad ; \quad M \equiv +1 \pmod 3 \quad ; \quad 1 \equiv M(1\cdot 2\cdot 3\ldots m)^3 \pmod n$$

Si se hace $3x+1 = y$, entonces resulta $y^3 - 3ny - Mn = 0$.

Reducción a ecuaciones puras de las ecuaciones que dan las raíces Ω.

359.

Las investigaciones precedentes trataban del *descubrimiento* de ecuaciones auxiliares. Ahora explicaremos una propiedad muy notable concerniente a sus *soluciones.* Consta que todos los trabajos de los geómetras eminentes han fracasado en la búsqueda de una solución general de ecuaciones de grado mayor que cuatro, o (para definir lo que se desea más exactamente) de la REDUCCION DE ECUACIONES MIXTAS A ECUACIONES PURAS. Existe la pequeña duda de si este problema no solamente está más allá de las facultades del análisis contemporáneo sino que propone lo imposible (cf. lo que dijimos de este asunto en *Demonstr. nova etc., art.* 9). No obstante es cierto que existen innumerables ecuaciones mixtas de todos los grados que admiten una reducción a ecuaciones puras, y esperamos que los geómetras encontrarán esto gratificante si demostramos que nuestras ecuaciones son siempre de esta clase. Pero a causa de la longitud de esta discusión, presentaremos aquí solamente los principios más importantes para demostrar que la reducción es posible; reservamos para otra ocasión una consideración más completa, la que el tema merece. Presentaremos primero algunas observaciones generales acerca de las raíces de la ecuación $x^e - 1 = 0$, la que también abarca el caso en que e es un número compuesto.

I. Estas raíces están dadas (como se sabe de los libros elementales) por $\cos \frac{kP}{e} + i \operatorname{sen} \frac{kP}{e}$, donde para k tomamos los e números $0, 1, 2, 3, \ldots e-1$ o cualesquiera otros que sean congruentes a éstos según el módulo e. Una raíz, para $k = 0$ o para cualquier k divisible por e será $= 1$. Para cualquier otro valor de k será una raíz que es diferente de 1.

II. Puesto que $(\cos \frac{kP}{e} + i \operatorname{sen} \frac{kP}{e})^\lambda = \cos \frac{\lambda kP}{e} + i \operatorname{sen} \frac{\lambda kP}{e}$, es claro que si R es una tal raíz correspondiente a un valor de k que es primo relativo a e, entonces en la progresión R, R^2, R^3, etc., el e-ésimo término será $= 1$ y todos los valores antecedentes son diferentes de 1. Se sigue inmediatamente que todas las e cantidades 1, R, R^2, R^3, $\ldots R^{e-1}$ son diferentes y, ya que todas ellas satisfacen la ecuación $x^e - 1 = 0$, ellas darán todas las raíces de esta ecuación.

III. Finalmente, bajo la misma suposición, la suma

$$1 + R^\lambda + R^{2\lambda} \cdots + R^{\lambda(e-1)} = 0$$

para cualquier valor del entero λ no divisible por e. Por esto es $= \frac{1-R^{\lambda e}}{1-R^\lambda}$ y el numerador de esta fracción es $= 0$, pero el denominador no es $= 0$. Cuando λ es divisible por e, la suma obviamente $= e$.

360.

Sea n, como siempre, un número primo, g una raíz primitiva para el módulo n, y $n-1$ el producto de tres enteros positivos α, β y γ. Por brevedad incluiremos en éste los casos en que α o $\gamma = 1$. Cuando $\gamma = 1$, reemplazamos las sumas $(\gamma, 1)$, (γ, g), etc. por las raíces $[1]$, $[g]$, etc. Supongamos por lo tanto que todas las α sumas de $\beta\gamma$ términos $(\beta\gamma, 1)$, $(\beta\gamma, g)$, $(\beta\gamma, g^2)$ y $(\beta\gamma, g^{\alpha-1})$ son conocidas y que queremos encontrar las sumas de γ términos. Hemos reducido la operación anterior a una ecuación mixta de grado β. Ahora mostraremos como resolverla mediante una ecuación pura del mismo grado. Por brevedad en vez de las sumas

$$(\gamma, 1),\ (\gamma, g^{\alpha}),\ (\gamma, g^{2\alpha}),\ \ldots (\gamma, g^{\alpha\beta-\alpha})$$

los cuales están contenidas en $(\beta, \gamma, 1)$, escribiremos a, b, c, $\ldots m$ respectivamente. En vez de las sumas

$$(\gamma, g),\ (\gamma, g^{\alpha+1}),\ \ldots (\gamma, g^{\alpha\beta-\alpha+1})$$

contenidas en $(\beta\gamma, g)$ escribiremos a', b', $\ldots m'$. Y en vez de

$$(\gamma, g^2),\ (\gamma, g^{\alpha+2}),\ \ldots (\gamma, g^{\alpha\beta-\alpha+2})$$

escribiremos a'', b'', $\ldots m''$, etc. hasta que se llegue a aquéllas que están contenidas en $(\beta\gamma, g^{\alpha-1})$.

I. Sea R una raíz arbitraria de la ecuación $x^{\beta} - 1 = 0$ y supongamos que la potencia de grado β de la función

$$t = a + Rb + R^2c + \cdots + R^{\beta-1}m$$

es, de acuerdo con las reglas del artículo 345,

$$\begin{aligned} N &+ Aa + Bb + Cc \cdots + Mm \\ &+ A'a' + B'b' + C'c' \cdots + M'm' \\ &+ A''a'' + B''b'' + C''c'' \cdots + M''m'' \\ &+ \text{ etc.} \qquad\qquad\qquad\qquad\qquad\qquad = T \end{aligned}$$

donde todos los coeficientes N, A, B, A', etc. son funciones racionales enteras de R. Supónganse también que las β-ésimas potencias de las otras dos funciones

$$u = R^{\beta}a + Rb + R^2c \cdots + R^{\beta-1}m \qquad \text{y} \qquad u' = b + Rc + R^2d \cdots + R^{\beta-2}m + R^{\beta-1}a$$

se hacen respectivamente U y U'. Es fácil ver del artículo 350 que, puesto que u' resulta de reemplazar las sumas a, b, c, $\ldots m$ con b, c, d, $\ldots a$, tenemos

$$\begin{aligned} U' = {} & N + Ab + Bc + Cd \cdots + Ma \\ & + A'b' + B'c' + C'd' \cdots + M'a' \\ & + A''b'' + B''c'' + C''d'' \cdots + M''a'' \\ & + \text{ etc.} \end{aligned}$$

También es claro que $u = Ru'$ y luego $U = R^\beta U'$. Ya que $R^\beta = 1$, los coeficientes correspondientes en U y U' serán iguales. Finalmente, ya que t y u difieren solamente en cuanto a que a se multiplica por la unidad en t y por R^β en u, todos los coeficientes correspondientes (i.e., aquéllos que multiplican las mismas sumas) en T y en U, serán iguales, y así también los coeficientes correspondientes en T y en U'. Por lo tanto $A = B = C$ etc. $= M$; $A' = B' = C'$ etc.; $A'' = B'' = C''$ etc.; en T se reduce a una forma como

$$N + A(\beta\gamma, 1) + A'(\beta\gamma, g) + A''(\beta\gamma, g^2) + \text{ etc.}$$

donde los coeficientes individuales N, A, A', etc. son de la forma

$$pR^{\beta-1} + p'R^{\beta-2} + p''R^{\beta-3} + \text{ etc.}$$

de tal forma que p, p', p'', etc. son enteros dados.

II. Si se toma por R una raíz determinada de la ecuación $x^\beta - 1 = 0$ (suponemos que ya tenemos sus soluciones) de tal manera que ninguna potencia menor que la β-ésima potencia es igual a la unidad, T también será una cantidad determinada, y de esto es posible derivar t mediante la ecuación pura $t^\beta - T = 0$. Pero, puesto que esta ecuación tiene β raíces que son t, Rt, R^2t, $\ldots R^{\beta-1}t$, puede existir una duda sobre cual de las raíces debe ser escogida. Sin embargo, esto es arbitrario como se mostrará. Recuérdese que, después de que todas las sumas de $\beta\gamma$ términos están determinadas, la raíz [1] se define como cualquiera de las $\beta\gamma$ raíces contenidas en $(\beta\gamma, 1)$, que luego debe ser denotada por este símbolo. Así es completamente arbitrario cual de las β sumas que conforman $(\beta\gamma, 1)$ queremos designar por a. Si después de que una de estas sumas se expresa por a, se supone que $t = \mathfrak{T}$, es fácil ver que la suma que se designaba por b puede ser cambiada a a y lo que anteriormente fue c, d, $\ldots a$, b ahora se convierte en b, c, $\ldots m$, a, y el valor de t es ahora $= \frac{\mathfrak{T}}{R} = \mathfrak{T}R^{\beta-1}$.

Similarmente, si conviene hacer a igual a la suma que en un principio fue c, el valor de t se convierte en $\mathfrak{T}R^{\beta-2}$ y así sucesivamente. Así, t puede considerarse igual a cualquiera de las cantidades $\mathfrak{T}$, $\mathfrak{T}R^{\beta-1}$, $\mathfrak{T}R^{\beta-2}$, etc., i.e., a cualquier raíz de la ecuación $x^\beta - T = 0$, de acuerdo con que una u otra de las sumas en $(\beta\gamma, 1)$ sea expresada por $(\gamma, 1)$. *Q. E. D.*

III. Después de que la cantidad t ha sido determinada de esta forma, hay que determinar las otras $\beta - 1$ que resultan de t sustituyendo R sucesivamente por R^2, R^3, R^4, $\ldots R^\beta$, esto es

$$t' = a + R^2 b + R^4 c \cdots + R^{2\beta-2} m, \qquad t'' = a + R^3 b + R^6 c \cdots + R^{3\beta-3} m, \quad \text{etc.}$$

La última de éstas ya se conoce, porque ella evidentemente $= a + b + c \cdots + m = (\beta\gamma, 1)$; las otras pueden encontrarse de la siguiente forma. Por los preceptos del artículo 345 se puede encontrar el producto $t^{\beta-2}t'$ tal como t^β en I. Entonces usamos un método tal como el precedente para mostrar que de esto, se puede reducir a una forma

$$\mathfrak{N} + \mathfrak{A}(\beta\gamma, 1) + \mathfrak{A}'(\beta\gamma, g) + \mathfrak{A}''(\beta\gamma, g^2) \text{ etc.} = T'$$

donde $\mathfrak{N}$, $\mathfrak{A}$, $\mathfrak{A}'$, etc. son funciones racionales enteras de R y así T' es una cantidad conocida y $t' = \frac{T't^2}{T}$. Exactamente de la misma manera se encuentra T'' por el cálculo del producto $t^{\beta-3}t''$. Esta expresión tendrá una forma similar y puesto que su valor es conocido se deriva la ecuación $t'' = \frac{T''t^3}{T}$. Entonces t''' puede ser encontrado de la ecuación $t''' = \frac{T'''t^4}{T}$ donde T''' es asimismo una cantidad conocida, etc.

Este método no sería aplicable si fuera $t = 0$, porque entonces $T = T' = T''$ etc. $= 0$. Pero se puede mostrar que esto es imposible, aunque la demostración es tan larga que es necesario omitirla aquí. También existen algunos artificios especiales para convertir las fracciones $\frac{T'}{T}$, $\frac{T''}{T}$, etc. en funciones racionales *enteras* de R y algunos métodos más cortos, en el caso donde $\alpha = 1$, para encontrar los valores de t', t'', etc., pero no los consideramos aquí.

IV. Finalmente, una vez encontrados t, t', t'', etc., observando III del artículo precedente, resulta inmediatamente que $t + t' + t'' +$ etc. $= \beta a$. Esto da el valor de a y de esto, por el artículo 346, se pueden derivar los valores de todas las restantes sumas de γ términos. Los valores de b, c, d, etc. también pueden ser encontrados, como lo mostrará una pequeña investigación, de las ecuaciones siguientes:

$$\beta b = R^{\beta-1}t + R^{\beta-2}t' + R^{\beta-3}t'' + \text{ etc.}$$
$$\beta c = R^{2\beta-2}t + R^{2\beta-4}t' + R^{2\beta-6}t'' + \text{ etc.}$$
$$\beta d = R^{3\beta-3}t + R^{3\beta-6}t' + R^{3\beta-9}t'' + \text{ etc., etc.}$$

Entre el gran número de observaciones que podemos hacer concernientes a la discusión precedente enfatizamos solamente una. Con respecto a la solución de la ecuación pura $x^\beta - T = 0$, es claro que en muchos casos T tiene el valor imaginario $P + iQ$, así la solución depende en parte de la división de un ángulo (cuya tangente $= \frac{Q}{P}$), en parte de la división de una razón (uno a $\sqrt{P^2+Q^2}$) en β partes. Es notable (no proseguiremos con este tema aquí) que el valor de $\sqrt[\beta]{P^2+Q^2}$ siempre puede ser expresado *racionalmente* mediante cantidades ya conocidas. Así, excepto por la extracción de una raíz cuadrada, la *única* cosa que se requiere para una solución es la división del ángulo, e.g., para $\beta = 3$ solamente la trisección de un ángulo.

Finalmente, puesto que nada nos impide hacer $\alpha = 1$, $\gamma = 1$ y de este modo $\beta = n - 1$, es evidente que la solución de la ecuación $x^n - 1 = 0$ puede ser reducida inmediatamente a la solución de una ecuación pura $x^{n-1} - T = 0$ de grado $n-1$. Aquí T se determinará por las raíces de la ecuación $x^{n-1} - 1 = 0$. Como un resultado, la división del círculo completo en n partes requiere, 1^o, la división del círculo completo en $n-1$ partes; 2^o, la división de otro arco en $n-1$ partes, el cual puede ser construido tan pronto como la primera división esté hecha; 3^o, la extracción de una raíz cuadrada y se puede mostrar que siempre es $\sqrt{n}$.

Aplicación de lo anterior a funciones trigonométricas.
Método para encontrar los ángulos de raíces particulares en Ω.

361.

Falta examinar más de cerca la conexión entre las raíces Ω y las funciones trigonométricas de los ángulos $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, $\ldots$ $\frac{(n-1)P}{n}$. El método usado para encontrar las raíces de Ω (a menos que consultemos tablas de senos, pero esto sería menos directo) deja incierto *cuales* raíces corresponden a los ángulos *individuales*; i.e., cuál raíz $= \cos\frac{P}{n} + i\,\mathrm{sen}\,\frac{P}{n}$, cual $= \cos\frac{2P}{n} + i\,\mathrm{sen}\,\frac{2P}{n}$, etc. Pero esta incertidumbre se puede eliminar fácilmente reflexionando que los cosenos de los ángulos $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, $\ldots$ $\frac{(n-1)P}{2n}$ están decreciendo continuamente (tomando en cuenta los signos) y que los senos son positivos. Por otro lado los ángulos $\frac{(n-1)P}{n}$, $\frac{(n-2)P}{n}$, $\frac{(n-3)P}{n}$, $\ldots$ $\frac{(n+1)P}{2n}$ tienen los mismos cosenos que los de antes, pero los senos son negativos, aunque tienen los mismos valores absolutos. Por lo tanto, de las raíces Ω, las dos que tienen la mayor parte real (son iguales una a la otra) corresponden a los ángulos $\frac{P}{n}$, $\frac{(n-1)P}{n}$. La primera tiene positivo el coeficiente de i, la segunda lo tiene negativo. De las $n-3$ raíces restantes, aquéllas que tienen la mayor parte real corresponden a los ángulos

$\frac{2P}{n}$, $\frac{(n-2)P}{n}$, y así sucesivamente. En tanto que se conozca la raíz correspondiente al ángulo $\frac{P}{n}$, las correspondientes a los restantes ángulos se pueden determinar a partir de ella porque, si suponemos que es $= [\lambda]$, las raíces $[2\lambda]$, $[3\lambda]$, $[4\lambda]$, etc. corresponderán a los ángulos $\frac{2P}{n}$, $\frac{3P}{n}$, $\frac{4P}{n}$, etc. Así en el ejemplo del artículo 353 vemos que la raíz correspondiente al ángulo $\frac{1}{19}P$ debe ser [11] y [8] la del ángulo $\frac{18}{19}P$. Similarmente las raíces [3], [16], [14], [5], etc. corresponderán a los ángulos $\frac{2}{19}P$, $\frac{17}{19}P$, $\frac{3}{19}P$, $\frac{16}{19}P$, etc. En el ejemplo del artículo 354 la raíz [1] corresponderá al ángulo $\frac{1}{17}P$, [2] al ángulo $\frac{2}{17}P$, etc. De esta forma los cosenos y senos de los ángulos $\frac{P}{n}$, $\frac{2P}{n}$, etc. serán completamente determinados.

Se derivan tangentes, cotangentes, secantes y cosecantes a partir de senos y cosenos sin división.

362.

Con respecto a los restantes funciones trigonométricas de estos ángulos, pudieron, por supuesto, derivarse de los cosenos y senos correspondientes mediante métodos ordinarios bien conocidos. Así secantes y tangentes se pueden encontrar dividiendo respectivamente la unidad y el seno por el coseno; cosecantes y cotangentes dividiendo la unidad y el coseno por el seno. Pero a menudo será mucho más útil obtener las mismas cantidades con la ayuda de las siguientes fórmulas, usando sólo adición y ninguna división. Sea ω uno cualquiera de los ángulos $\frac{P}{n}$, $\frac{2P}{n}$, $\ldots$ $\frac{(n-1)P}{n}$ y sea $\cos\omega + i\,\mathrm{sen}\,\omega = R$, de modo que R será una de las raíces Ω, entonces

$$\cos\omega = \frac{1}{2}(R + \frac{1}{R}) = \frac{1+R^2}{2R}, \qquad \mathrm{sen}\,\omega = \frac{1}{2i}(R - \frac{1}{R}) = \frac{i(1-R^2)}{2R}$$

y de esto

$$\sec\omega = \frac{2R}{1+R^2}, \quad \tan\omega = \frac{i(1-R^2)}{1+R^2}, \quad \csc\omega = \frac{2Ri}{R^2-1}, \quad \cot\omega = \frac{i(R^2+1)}{R^2-1}$$

Ahora mostraremos como transformar los numeradores de estas cuatro fracciones de modo que sean divisibles por los denominadores.

I. Ya que $R = R^{n+1} = R^{2n+1}$ tenemos $2R = R + R^{2n+1}$. Esta expresión es divisible por $1 + R^2$ pues n es un número impar. Así tenemos

$$\sec\omega = R - R^3 + R^5 - R^7 \cdots + R^{2n-1}$$

y así (puesto que $\operatorname{sen}\omega = -\operatorname{sen}(2n-1)\omega$, $\operatorname{sen}3\omega = -\operatorname{sen}(2n-3)\omega$ etc. tenemos $\operatorname{sen}\omega - \operatorname{sen}3\omega + \operatorname{sen}5\omega \cdots + \operatorname{sen}(2n-1)\omega = 0$)

$$\sec\omega = \cos\omega - \cos 3\omega + \cos 5\omega \cdots + \cos(2n-1)\omega$$

o finalmente (ya que $\cos\omega = \cos(2n-1)\omega$, $\cos 3\omega = \cos(2n-3)\omega$, etc.)

$$= 2(\cos\omega - \cos 3\omega + \cos 5\omega \cdots \mp \cos(n-2)\omega) \pm \cos n\omega$$

los signos superiores o inferiores se tomarán de acuerdo con que n sea de la forma $4k+1$ o $4k+3$. Obviamente esta fórmula también se puede expresar como

$$\sec\omega = \pm\Big(1 - 2\cos 2\omega + 2\cos 4\omega \cdots \pm 2\cos(n-1)\omega\Big)$$

II. Similarmente, sustituyendo $1 - R^2$ por $1 - R^{2n+2}$ resulta

$$\tan\omega = i(1 - R^2 + R^4 - R^6 \cdots - R^{2n})$$

o (ya que $1 - R^{2n} = 0$, $R^2 - R^{2n-2} = 2i\operatorname{sen}2\omega$, $R^4 - R^{2n-4} = 2i\operatorname{sen}4\omega$, etc.)

$$\tan\omega = 2\Big(\operatorname{sen}2\omega - \operatorname{sen}4\omega + \operatorname{sen}6\omega \cdots \mp \operatorname{sen}(n-1)\omega\Big)$$

III. Puesto que $1 + R^2 + R^4 \cdots + R^{2n-2} = 0$, tenemos

$$\begin{aligned} n &= n - 1 - R^2 - R^4 \cdots - R^{2n-2} \\ &= (1-1) + (1-R^2) + (1-R^4) \cdots + (1-R^{2n-2}) \end{aligned}$$

y cada uno de sus términos es divisible por $1 - R^2$. Así

$$\begin{aligned} \frac{n}{1-R^2} &= 1 + (1+R^2) + (1+R^2+R^4) \cdots + (1+R^2+R^4 \cdots + R^{2n-4}) \\ &= (n-1) + (n-2)R^2 + (n-3)R^4 \cdots + R^{2n-4} \end{aligned}$$

Multiplicando por 2 y restando la cantidad

$$0 = (n-1)(1 + R^2 + R^4 \cdots + R^{2n-2})$$

y asimismo multiplicando por R tenemos

$$\frac{2nR}{1-R^2} = (n-1)R + (n-3)R^3 + (n-5)R^5 \cdots - (n-3)R^{2n-3} - (n-1)R^{2n-1}$$

y de esto inmediatamente obtenemos

$$\csc\omega = \frac{1}{n}\Big((n-1)\operatorname{sen}\omega + (n-3)\operatorname{sen}3\omega \cdots - (n-1)\operatorname{sen}(2n-1)\omega\Big)$$
$$= \frac{2}{n}\Big((n-1)\operatorname{sen}\omega + (n-3)\operatorname{sen}3\omega + \text{ etc.} + 2\operatorname{sen}(n-2)\omega\Big)$$

Esta fórmula puede ser expresada también como

$$\csc\omega = -\frac{2}{n}\Big(2\operatorname{sen}2\omega + 4\operatorname{sen}4\omega + 6\operatorname{sen}6\omega \cdots + (n-1)\operatorname{sen}(n-1)\omega\Big)$$

IV. Multiplicando el valor de $\frac{n}{1-R^2}$, dado antes, por $1+R^2$ y restando la cantidad

$$0 = (n-1)(1 + R^2 + R^4 \cdots + R^{2n-2})$$

tenemos

$$\frac{n(1+R^2)}{1-R^2} = (n-2)R^2 + (n-4)R^4 + (n-6)R^6 \cdots - (n-2)R^{2n-2}$$

y de esto sigue inmediatamente que

$$\cot\omega = \frac{1}{n}\Big((n-2)\operatorname{sen}2\omega + (n-4)\operatorname{sen}4\omega + (n-6)\operatorname{sen}6\omega \cdots - (n-2)\operatorname{sen}(n-2)\omega\Big)$$
$$= \frac{2}{n}\Big((n-2)\operatorname{sen}2\omega + (n-4)\operatorname{sen}4\omega \cdots + 3\operatorname{sen}(n-3)\omega + \operatorname{sen}(n-1)\omega\Big)$$

y esta fórmula también se puede expresar como

$$\cot\omega = -\frac{2}{n}\Big(\operatorname{sen}\omega + 3\operatorname{sen}3\omega \cdots + (n-2)\operatorname{sen}(n-2)\omega\Big)$$

Método de reducir sucesivamente las ecuaciones para funciones trigonométricas.

363.

Suponiendo otra vez que $n-1 = ef$, la función X puede ser resuelta en e factores de grado f en tanto que se sepan los valores de todas las e sumas de f términos (art. 338). De la misma manera, suponiendo que $Z=0$ es una ecuación de grado $n-1$ cuyas raíces son los senos o cualquiera otra función trigonométrica de los

ángulos $\frac{P}{n}$, $\frac{2P}{n}$ $\ldots$ $\frac{(n-1)P}{n}$, la función Z se puede resolver en e factores de grado f de la siguiente forma.

Sea Ω el conjunto de los e períodos de f términos $(f,1) = P$, P', P'', etc. Sea P el período de las raíces $[1]$, $[a]$, $[b]$, $[c]$, etc.; P' el de las raíces $[a']$, $[b']$, $[c']$, etc.; P'' el de las raíces $[a'']$, $[b'']$, $[c'']$, etc., etc. Sea el ángulo ω correspondiente a la raíz $[1]$, y así los ángulos $a\omega$, $b\omega$, etc. a las raíces $[a]$, $[b]$, etc.; los ángulos $a'\omega$, $b'\omega$, etc. a las raíces $[a']$, $[b']$, etc.; los ángulos $a''\omega$, $b''\omega$, etc. a las raíces $[a'']$, $[b'']$, etc. Es fácil ver que todos estos ángulos tomados juntos coinciden, con respecto a sus funciones trigonométricas*), con los ángulos $\frac{P}{n}$, $\frac{2P}{n}$, $\frac{3P}{n}$, $\ldots$ $\frac{(n-1)P}{n}$. Ahora si se denota la función que se trata por el carácter φ prefijado al ángulo, y si Y es el producto de los e factores

$$x - \varphi\omega, \quad x - \varphi a\omega, \quad x - \varphi b\omega \text{ etc.}$$

y el producto de los factores $x - \varphi a'\omega$, $x - \varphi b'\omega$, etc. $= Y'$, el producto de $x - \varphi a''\omega$, $x - \varphi b''\omega$, etc. $= Y''$ etc.: entonces necesariamente el producto $YY'Y''\cdots = Z$. Resta ahora mostrar que todos los coeficientes en las funciones Y, Y', Y'', etc. pueden ser reducidos a la forma

$$A + B(f,1) + C(f,g) + D(f,g^2)\cdots + L(f,g^{e-1})$$

Hecho esto, evidentemente todos ellos serán conocidos en tanto se conozcan los valores de todas las sumas de f términos: mostramos esto de la siguiente forma.

Tal como $\cos\omega = \frac{1}{2}[1] + \frac{1}{2}[1]^{n-1}$, $\operatorname{sen}\omega = -\frac{1}{2}i[1] + \frac{1}{2}i[1]^{n-1}$ así por el artículo precedente todas las restantes funciones trigonométricas del ángulo ω se pueden reducir a la forma $\mathfrak{A} + \mathfrak{B}[1] + \mathfrak{C}[1]^2 + \mathfrak{D}[1]^3 +$ etc. y no es difícil ver que la función del ángulo $k\omega$ se hace $= \mathfrak{A} + \mathfrak{B}[k] + \mathfrak{C}[k]^2 + \mathfrak{D}[k]^3 +$ etc. donde k es cualquier entero. Ahora, puesto que los coeficientes individuales en Y son funciones racionales enteras invariables de $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$, etc., si se sustituyen sus valores por estas cantidades, sus coeficientes individuales se convertirán en funciones racionales enteras invariables de $[1]$, $[a]$, $[b]$, etc. Por lo tanto, por el artículo 347, ellas se reducirán a la forma $A + B(f,1) + C(f,g) +$ etc. Los coeficientes en Y', Y'', etc. también pueden ser reducidos a formas similares. *Q. E. D.*

---

*) Dos ángulos coinciden en este aspecto si su diferencia es igual a la circunferencia o a un múltiplo de ella. Podemos decir que son *congruentes según la circunferencia* si queremos usar el término congruencia en un sentido extendido

364.

Agregamos unas pocas observaciones acerca del problema del artículo precedente.

I. Los coeficientes individuales en Y' son funciones de raíces contenidas en el período $P' = (f, a')$ tal como las funciones de las raíces en P dan los coeficientes correspondientes en Y. Es claro del artículo 347, por lo tanto, que se puede derivar Y' de Y, sustituyendo en todo lugar en Y las cantidades $(f, 1)$, (f, g), (f, g^2), etc. por (f, a'), $(f, a'g)$, $(f, a'g^2)$, etc. respectivamente. Igualmente Y'' puede ser derivado de Y, sustituyendo en todo lugar en Y las cantidades $(f, 1)$, (f, g), (f, g^2), etc. por (f, a''), $(f, a''g)$, $(f, a''g^2)$, etc. respectivamente, etc. Por consiguiente, en tanto que se tenga la función Y, las restantes Y', Y'', etc. siguen fácilmente.

II. Suponiendo

$$Y = x^f - \alpha x^{f-1} + \beta x^{f-2} - \text{ etc.}$$

los coeficientes α, β, etc. son respectivamente la suma de las raíces de la ecuación $Y = 0$, i.e., de las cantidades $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$, etc., la suma de sus productos tomados dos a dos, etc. Pero a menudo estos coeficientes se encontrarán mucho más cómodamente por un método similar al del artículo 349, esto es, calculando la suma de las raíces $\varphi\omega$, $\varphi a\omega$, $\varphi b\omega$, etc., la suma de sus cuadrados, cubos, etc. y deduciendo de esto por el teorema de Newton esos coeficientes. Siempre que φ designe la tangente, secante, cotangente o cosecante se dan aún otros métodos de abreviación del proceso, pero no podemos considerarlos aquí.

III. El caso donde f es un número par merece consideración especial porque entonces cada uno de los períodos P, P', P'', etc. estará compuesto de $\frac{1}{2}f$ períodos de dos términos. Si P consiste de los períodos $(2, 1)$, $(2, \mathfrak{a})$, $(2, \mathfrak{b})$, $(2, \mathfrak{c})$, etc., entonces los números 1, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, etc. y $n-1$, $n-\mathfrak{a}$, $n-\mathfrak{b}$, $n-\mathfrak{c}$, etc. tomados en conjunto coincidirán con los números 1, a, b, c, etc. o al menos (esto viene a ser la misma cosa) serán congruentes a ellos según el módulo n. Pero $\varphi(n-1)\omega = \pm\varphi\omega$, $\varphi(n-\mathfrak{a})\omega = \pm\varphi\mathfrak{a}\omega$ etc., donde los signos superiores son tomados cuando φ designa el coseno o la secante, los inferiores cuando φ designa el seno, la tangente, la cotangente o la cosecante. Se sigue de esto que en los dos primeros casos, los factores que componen Y serán iguales dos a dos, y así Y es un cuadrado y será $= y^2$ si y se pone igual al producto de

$$x - \varphi\omega, \quad x - \varphi\mathfrak{a}\omega, \quad x - \varphi\mathfrak{b}\omega \text{ etc.}$$

En los mismos casos, las funciones restantes Y', Y'', etc. serán cuadrados, y suponiendo que P' está compuesto de $(2, \mathfrak{a}')$, $(2, \mathfrak{b}')$, $(2, \mathfrak{c}')$, etc.; P'' de $(2, \mathfrak{a}'')$, $(2, \mathfrak{b}'')$, $(2, \mathfrak{c}'')$, etc., etc., el producto de $x - \varphi\mathfrak{a}'\omega$, $x - \varphi\mathfrak{b}'\omega$, $x - \varphi\mathfrak{c}'\omega$, etc. $= y'$, el producto de $x - \varphi\mathfrak{a}''\omega$, $x - \varphi\mathfrak{b}''\omega$, etc. $= y''$, etc., entonces $Y' = y'^2$, $Y'' = y''^2$, etc.; y la función Z también será un cuadrado (cf. antes, art. 337) y sus raíces serán iguales al producto de y, y', y'', etc. Pero claramente y', y'', etc. pueden ser derivadas de y tal como dijimos en I que Y', Y'' son derivadas de Y. Luego, los coeficientes individuales en y también pueden ser reducidos a la forma

$$A + B(f, 1) + C(f, g) + \text{ etc.}$$

porque las sumas de las potencias individuales de las raíces de la ecuación $y = 0$ son iguales a la mitad de las sumas de las potencias de las raíces de la ecuación $y = 0$ y así son reducibles a una forma tal. En los cuatro casos posteriores sin embargo, Y será el producto de los factores

$$x^2 - (\varphi\omega)^2,\ x^2 - (\varphi\mathfrak{a}\omega)^2,\ x^2 - (\varphi\mathfrak{b}\omega)^2 \text{ etc.}$$

y así de la forma

$$x^f - \lambda x^{f-2} + \mu x^{f-4} - \text{ etc.}$$

Es claro que los coeficientes λ, μ, etc. pueden ser deducidos de las sumas de cuadrados, bicuadrados, etc. de las raíces $\varphi\omega$, $\varphi\mathfrak{a}\omega$, $\varphi\mathfrak{b}\omega$, etc. La misma cosa es cierta para las funciones Y', Y'', etc.

Ejemplo. I. Sea $n = 17$, $f = 8$ y φ el coseno. Entonces resulta

$$Z = (x^8 + \frac{1}{2}x^7 - \frac{7}{4}x^6 - \frac{3}{4}x^5 + \frac{15}{16}x^4 + \frac{5}{16}x^3 - \frac{5}{32}x^2 - \frac{1}{32}x + \frac{1}{256})^2$$

y así $\sqrt{Z}$ será resuelta en dos factores y, y' de grado cuatro. El período $P = (8, 1)$ consiste de $(2, 1)$, $(2, 9)$, $(2, 13)$ y $(2, 15)$; así y será un producto de los factores

$$x - \varphi\omega, \quad x - \varphi 9\omega, \quad x - \varphi 13\omega, \quad x - \varphi 15\omega$$

Sustituyendo $\varphi k\omega$ por $\frac{1}{2}[k] + \frac{1}{2}[n - k]$ se encuentra que

$$\varphi\omega + \varphi 9\omega + \varphi 13\omega + \varphi 15\omega = \frac{1}{2}(8, 1)$$
$$(\varphi\omega)^2 + (\varphi 9\omega)^2 + (\varphi 13\omega)^2 + (\varphi 15\omega)^2 = 2 + \frac{1}{4}(8, 1)$$

Asimismo la suma de los cubos es $= \frac{3}{8}(8,1) + \frac{1}{8}(8,3)$ y la suma de los bicuadrados es $= 1\frac{1}{2} + \frac{5}{16}(8,1)$. Así por el teorema de Newton los coeficientes en y serán

$$y = x^4 - \frac{1}{2}(8,1)x^3 + \frac{1}{4}\Big((8,1) + 2(8,3)\Big)x^2 - \frac{1}{8}\Big((8,1) + 3(8,3)\Big)x + \frac{1}{16}\Big((8,1) + (8,3)\Big)$$

e y' es derivado de y intercambiando $(8,1)$ y $(8,3)$. Por lo tanto sustituyendo $(8,1)$ y $(8,3)$ por los valores $-\frac{1}{2} + \frac{1}{2}\sqrt{17}$ y $-\frac{1}{2} - \frac{1}{2}\sqrt{17}$, obtenemos

$$y = x^4 + (\frac{1}{4} - \frac{1}{4}\sqrt{17})x^3 - (\frac{3}{8} + \frac{1}{8}\sqrt{17})x^2 + (\frac{1}{4} + \frac{1}{8}\sqrt{17})x - \frac{1}{16}$$
$$y' = x^4 + (\frac{1}{4} + \frac{1}{4}\sqrt{17})x^3 - (\frac{3}{8} - \frac{1}{8}\sqrt{17})x^2 + (\frac{1}{4} - \frac{1}{8}\sqrt{17})x - \frac{1}{16}$$

Similarmente $\sqrt{Z}$ se puede resolver en cuatro factores de grado dos. El primero será $(x - \varphi\omega)(x - \varphi 13\omega)$, el segundo $(x - \varphi 9\omega)(x - \varphi 15\omega)$, el tercero $(x - \varphi 3\omega)(x - \varphi 5\omega)$, el cuarto $(x - \varphi 10\omega)(x - \varphi 11\omega)$, y todos los coeficientes en estos factores pueden ser expresados en términos de las cuatro sumas $(4,1)$, $(4,9)$, $(4,3)$ y $(4,10)$. Evidentemente el producto del primer factor por el segundo factor será y, el producto del tercero por el cuarto será y'.

Ejemplo. II. Si, con todo lo demás igual, se supone que φ representa el seno, de modo que

$$Z = x^{16} - \frac{17}{4}x^{14} + \frac{119}{16}x^{12} - \frac{221}{32}x^{10} + \frac{935}{256}x^8 - \frac{561}{512}x^6 + \frac{357}{2048}x^4 - \frac{51}{4096}x^2 + \frac{17}{65536}$$

ha de ser resuelto en dos factores y e y' de grado 8, entonces y será un producto de cuatro factores cuadrados

$$x^2 - (\varphi\omega)^2, \quad x^2 - (\varphi 9\omega)^2, \quad x^2 - (\varphi 13\omega), \quad x^2 - (\varphi 15\omega)^2$$

Ahora, ya que $\varphi k\omega = -\frac{1}{2}i[k] + \frac{1}{2}i[n-k]$, resulta

$$(\varphi k\omega)^2 = -\frac{1}{4}[2k] + \frac{1}{2}[n] - \frac{1}{4}[2n-2k] = \frac{1}{2} - \frac{1}{4}[2k] - \frac{1}{4}[2n-2k]$$

Así, la suma de los cuadrados de las raíces $\varphi\omega$, $\varphi 9\omega$, $\varphi 13\omega$, $\varphi 15\omega$ será $2 - \frac{1}{4}(8,1)$, la suma de sus cuartas potencias $= \frac{3}{2} - \frac{3}{16}(8,1)$, la suma de sus sextas potencias

$= \frac{5}{4} - \frac{9}{64}(8,1) - \frac{1}{64}(8,3)$, la suma de sus octavas potencias $\frac{35}{32} - \frac{27}{256}(8,1) - \frac{1}{32}(8,3)$. Por lo tanto

$$y = x^8 - \Big(2 - \frac{1}{4}(8,1)\Big)x^6 + \Big(\frac{3}{2} - \frac{5}{16}(8,1) + \frac{1}{8}(8,3)\Big)x^4 - \Big(\frac{1}{2} - \frac{9}{64}(8,1) + \frac{5}{64}(8,3)\Big)x^2 + \frac{1}{16} - \frac{5}{256}(8,1) + \frac{3}{256}(8,3)$$

e y' es determinado a partir de y intercambiando $(8,1)$ y $(8,3)$, así, sustituyendo los valores de estas sumas obtenemos

$$y = x^8 - (\frac{17}{8} - \frac{1}{8}\sqrt{17})x^6 + (\frac{51}{32} - \frac{7}{32}\sqrt{17})x^4 - (\frac{17}{32} - \frac{7}{64}\sqrt{17})x^2 + \frac{17}{256} - \frac{1}{64}\sqrt{17}$$
$$y' = x^8 - (\frac{17}{8} + \frac{1}{8}\sqrt{17})x^6 + (\frac{51}{32} + \frac{7}{32}\sqrt{17})x^4 - (\frac{17}{32} + \frac{7}{64}\sqrt{17})x^2 + \frac{17}{256} + \frac{1}{64}\sqrt{17}$$

Así Z puede ser resuelto en cuatro factores cuyos coeficientes se pueden expresar por sumas de cuatro términos. El producto de dos de ellos será y, el producto de los otros dos será y'.

Secciones del círculo que pueden realizarse por ecuaciones cuadráticas o sea por construcciones geométricas.

365.

Así, si n es un número primo, por la discusión precedente hemos reducido la división del círculo en n partes a la solución de tantas ecuaciones como factores haya en el número $n-1$. El grado de la ecuación se determina por el tamaño de los factores. Por lo tanto, siempre que $n-1$ es una potencia del número 2, lo que ocurre cuando el valor de n es 3, 5, 17, 257, 65537, etc., la división del círculo se reduce a ecuaciones cuadráticas únicamente, y las funciones trigonométricas de los ángulos $\frac{P}{n}$, $\frac{2P}{n}$, etc. pueden ser expresadas por raíces cuadradas que son más o menos complicadas (de acuerdo con el tamaño de n). Así, en estos casos la división del círculo en n partes o la inscripción de un polígono regular de n lados puede ser efectuada por construcciones geométricas. Así, e.g., para $n = 17$, por los artículos 354 y 361 se deriva la siguiente expresión para el coseno del ángulo $\frac{1}{17}P$:

$$-\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

El coseno de múltiplos de este ángulo tendrá una forma similar, pero el seno tendrá un signo radical más. Ciertamente es asombroso que aunque la divisibilidad geométrica del círculo en tres y cinco partes fue conocida ya en los tiempos de Euclides, nada fue agregado a este descubrimiento durante 2000 años. Todos los geómetras han asegurado que, excepto por aquellas secciones y las que se derivan directamente de ellas, esto es, división en 15, $3 \cdot 2^\mu$, $5 \cdot 2^\mu$, y 2^μ partes, no existen otras que puedan ser efectuadas por construcciones geométricas. Es fácil mostrar que si el número primo n es $= 2^m + 1$, el exponente m no puede tener otros factores primos excepto 2, y así es igual a 1 o 2 o una potencia mayor del número 2. Pues si m fuera divisible por algún número impar ζ (mayor que la unidad) de modo que $m = \zeta\eta$, entonces $2^m + 1$ sería divisible por $2^\eta + 1$ y así necesariamente compuesto. Todos los valores de n, que pueden ser reducidos a ecuaciones cuadráticas están, por consiguiente, contenidos en la forma $2^{2^\nu} + 1$. Así, los cinco números 3, 5, 17, 257, 65537 resultan de hacer $\nu = 0$, 1, 2, 3, 4 o $m = 1$, 2, 4, 8, 16. Pero la división geométrica del círculo no puede ser efectuada para *todos* los números contenidos en la fórmula sino solamente para aquéllos que son primos. Fermat fue engañado por su inducción y afirmó que todos los números contenidos en esa forma son necesariamente primos, pero el distinguido Euler notó primero que esta regla es errónea para $\nu = 5$ o sea $m = 32$, puesto que el número $2^{32} + 1 = 4294967297$ contiene el factor 641.

Siempre que $n-1$ contenga otros factores primos distintos de 2, somos llevados a ecuaciones de mayor grado, a saber, a una o más ecuaciones cúbicas cuando 3 aparece una o varias veces entre los factores primos de $n - 1$, a ecuaciones de quinto grado cuando $n-1$ es divisible por 5, etc., PODEMOS PROBAR CON TODO RIGOR QUE ESTAS ECUACIONES DE MAYOR GRADO NO PUEDEN SER ELUDIDAS DE NINGUNA FORMA NI PUEDEN SER REDUCIDAS A ECUACIONES DE MENOR GRADO. Los límites del presente trabajo excluyen aquí esta demostración, pero emitimos esta advertencia no sea que alguien intente llevar a cabo otras construcciones geométricas que no son las sugeridas por nuestra teoría (e.g., secciones en 7, 11, 13, 19, etc. partes) y así gaste su tiempo inútilmente.

366.

Si un círculo ha de ser cortado en a^α partes, donde a es un número primo, evidentemente esto puede ser hecho geométricamente cuando $a = 2$ pero no para cualquier otro valor de a si $\alpha > 1$, pues entonces además de las ecuaciones requeridas para la división en a partes, será necesario resolver otras $\alpha - 1$ de grado a, y éstas

no pueden ser evitadas ni reducidas de ninguna manera. Por lo tanto, en general, el grado de las ecuaciones necesarias se puede encontrar de los factores primos del número $(a-1)a^{\alpha-1}$ (incluyendo también el caso en que $\alpha = 1$).

Finalmente si el círculo ha de ser cortado en $N = a^\alpha b^\beta c^\gamma \ldots$ partes, donde a, b, c, etc. son números primos diferentes, es suficiente hacer divisiones en a^α, b^β, c^γ, etc. partes (art. 336). Así, a fin de conocer el grado de las ecuaciones necesarias para este propósito, es necesario considerar los factores primos de los números

$$(a-1)a^{\alpha-1}, \quad (b-1)b^{\beta-1}, \quad (c-1)c^{\gamma-1}, \text{ etc.}$$

o, lo que viene a ser la misma cosa, los factores de su producto. Se observa que este producto indica el número de enteros primos relativos a N y menores que él (art. 38). Geométricamente, por lo tanto, esta división puede ser realizada solamente cuando este número es una potencia de 2. Pero cuando los factores incluyen números primos diferentes de 2, digamos p, p', etc., entonces las ecuaciones de grados p, p', etc. no pueden ser evitadas. En general, por lo tanto, a fin de poder dividir geométricamente el círculo en N partes, N debe ser 2 o una potencia más alta de 2, *o* un número primo de la forma $2^m + 1$, *o* el producto de varios números primos de esta forma, *o* el producto de uno o varios de tales números primos por 2 o por una potencia más alta de 2. En resumen, se requiere que N no incluya factores primos impares que no sean de la forma $2^m + 1$ ni algún factor primo de la forma $2^m + 1$ más que una vez. Los siguientes son los 38 valores de N abajo de 300:
2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.

APENDICE.

Al art. 28. La solución de la ecuación indeterminada $ax = by \pm 1$ no fue encontrada primero por el ilustre Euler (como se consignó en esta Sección) sino por un geómetra del siglo diecisiete, Bachet de Meziriac, el célebre editor y comentador de Diofanto. Fue el ilustre Lagrange quien le restituyó este honor (*Add. à l'Algèbre d'Euler*, p. 525, donde a la vez indica el fondo del método). Bachet publicó su descubrimiento en la segunda edición del libro *Problèmes plaisans et délectables qui se font par les nombres*, 1624. En la primera edición (Lyon, 1612), que fue la única que vi, éste no fue incluido, aunque fue mencionado.

A los art. 151, 296, 297. El ilustre Legendre presentó su demostración nuevamente en su excelente trabajo, *Essai d'une théorie des nombres*, p. 214 y siguientes, pero no cambió nada esencial. Así, este método todavía está sujeto a las objecciones contenidas en el artículo 297. Es cierto que el teorema (sobre el cual se basa una suposición) que establece que cualquier progresión aritmética l, $l + k$, $l+2k$, etc. contiene números primos si k y l no tienen un divisor común, se expone más detalladamente en esta obra (p. 12 y siguientes), pero todavía no parece satisfacer el rigor geométrico. Pero aún si este teorema fuera enteramente demostrado, la segunda suposición permanece (que existen números primos de la forma $4n+3$ para los cuales un número positivo primo dado de la forma $4n+1$ es un no residuo cuadrático) y yo no sé si esto puede ser probado *rigurosamente* a menos que el teorema fundamental sea *asumido*. Pero debe observarse que Legendre no asumió tácitamente esta última suposición, ni intentó disimularla (p. 221).

A los art. 288–293. El mismo asunto presentado aquí como una aplicación de la teoría de formas ternarias, y que parece ser tan categórico con respecto al rigor y generalidad que nada más podría desearse, es tratado mucho más completamente por el ilustre Legendre en la tercera parte de su trabajo, pp. 321–400*). El usa principios y métodos muy diferentes de los nuestros, pero de esta forma encuentra muchas dificultades que le impiden proporcionar una demostración rigurosa a estos notables teoremas. El indica francamente estas dificultades, pero, a menos que yo esté equivocado, éstas pueden ser más fácilmente dispensadas con la suposición otra vez aquí del teorema cabalmente mencionado en la nota al pie de p. 371 (aquél que comienza "En cualquier progresión aritmética," etc.).

Al art. 306 VIII. En el tercer millar de determinantes negativos existen 37 que son irregulares; 18 de ellos tienen 2 como índice de irregularidad, los otros 19 índice 3.

Al art. 306 X. Recientemente hemos tenido éxito en resolver completamente las cuestiones propuestas aquí. Publicaremos muy pronto esta discusión en nuestra continuación del presente trabajo. Ella ilustra brillantemente muchas partes de la Aritmética y el Análisis superiores. La misma solución prueba que el coeficiente m en el artículo 304 es $= \gamma\pi = 2,3458847616$, donde γ es la misma cantidad que en el artículo 302 y π es la longitud de la mitad de la circunferencia de un círculo de radio 1.

---

*) El lector necesita ser escasamente advertido de que nuestras formas ternarias no deben ser confundidas con las que Lagrange llama *forme trinaire d'un nombre*. Por esta expresión él denota la descomposición de un número en tres cuadrados.

TABLAS

TABLA I. (artículos 58 y 91)

		2 . 3 . 5 . 7 . 11	13 . 17 . 19 . 23 . 29	31 . 37 . 41 . 43 . 47	53 . 59 . 61 . 67 . 71	73 . 79 . 83 . 89
3	2	1				
5	2	1 . 3				
7	3	2 . 1 . 5				
9	2	1 . * . 5 . 4				
11	2	1 . 8 . 4 . 7				
13	6	5 . 8 . 9 . 7 . 11				
16	5	* . 3 . 1 . 2 . 1	3			
17	10	10 . 11 . 7 . 9 . 13	12			
19	10	17 . 5 . 2 . 12 . 6	13 . 8			
23	10	8 . 20 . 15 . 21 . 3	12 . 17 . 5			
25	2	1 . 7 . * . 5 . 16	19 . 13 . 18 . 11			
27	2	1 . * . 5 . 16 . 13	8 . 15 . 12 . 11			
29	10	11 . 27 . 18 . 20 . 23	2 . 7 . 15 . 24			
31	17	12 . 13 . 20 . 4 . 29	23 . 1 . 22 . 21 . 27			
32	5	* . 3 . 1 . 2 . 5	7 . 4 . 7 . 6 . 3	0		
37	5	11 . 34 . 1 . 28 . 6	13 . 5 . 25 . 21 . 15	27		
41	6	26 . 15 . 22 . 39 . 3	31 . 33 . 9 . 36 . 7	28 . 32		
43	28	39 . 17 . 5 . 7 . 6	40 . 16 . 29 . 20 . 25	32 . 35 . 18		
47	10	30 . 18 . 17 . 38 . 27	3 . 42 . 29 . 39 . 43	5 . 24 . 25 . 37		
49	10	2 . 13 . 41 . * . 16	9 . 31 . 35 . 32 . 24	7 . 38 . 27 . 36 . 23		
53	26	25 . 9 . 31 . 38 . 46	28 . 42 . 41 . 39 . 6	45 . 22 . 33 . 30 . 8		
59	10	25 . 32 . 34 . 44 . 45	23 . 14 . 22 . 27 . 4	7 . 41 . 2 . 13 . 53	28	
61	10	47 . 42 . 14 . 23 . 45	20 . 49 . 22 . 39 . 25	13 . 33 . 18 . 41 . 40	51 . 17	
64	5	* . 3 . 1 . 10 . 5	15 . 12 . 7 . 14 . 11	8 . 9 . 14 . 13 . 12	5 . 1 . 3	
67	12	29 . 9 . 39 . 7 . 61	23 . 8 . 26 . 20 . 22	43 . 44 . 19 . 63 . 64	3 . 54 . 5	
71	62	58 . 18 . 14 . 33 . 43	27 . 7 . 38 . 5 . 4	13 . 30 . 55 . 44 . 17	59 . 29 . 37 . 11	
73	5	8 . 6 . 1 . 33 . 55	59 . 21 . 62 . 46 . 35	11 . 64 . 4 . 51 . 31	53 . 5 . 58 . 50 . 44	
79	29	50 . 71 . 34 . 19 . 70	74 . 9 . 10 . 52 . 1	76 . 23 . 21 . 47 . 55	7 . 17 . 75 . 54 . 33	4
81	11	25 . * . 35 . 22 . 1	38 . 15 . 12 . 5 . 7	14 . 24 . 29 . 10 . 13	45 . 53 . 4 . 20 . 33	48 . 52
83	50	3 . 52 . 81 . 24 . 72	67 . 4 . 59 . 16 . 36	32 . 60 . 38 . 49 . 69	13 . 20 . 34 . 53 . 17	43 . 47
89	30	72 . 87 . 18 . 7 . 4	65 . 82 . 53 . 31 . 29	57 . 77 . 67 . 59 . 34	10 . 45 . 19 . 32 . 26	68 . 46 . 27
97	10	86 . 2 . 11 . 53 . 82	83 . 19 . 27 . 79 . 47	26 . 41 . 71 . 44 . 60	14 . 65 . 32 . 51 . 25	20 . 42 . 91 . 18

TABLA II. (artículo 99)

	−1	+2	+3	+5	+7	+11	+13	+17	+19	+23	+29	+31	+37	+41	+43	+47	+53	+59	+61	+67	+71	+73	+79	+83	+89	+97
3			—		—		—		—			—	—		—				—	—		—	—			—
5	—			—		—			—		—	—		—				—	—		—		—		—	
7		—			—	—				—	—		—		—		—			—	—		—			
11			—	—		—				—		—	—			—	—	—			—				—	—
13	—		—				—	—		—	—				—		—		—				—			
17	—	—					—	—	—						—	—	—	—		—				—	—	
19				—	—	—		—	—	—					—	—			—			—		—		
23		—	—				—			—	—	—		—		—		—			—	—				
29	—			—	—		—			—	—						—	—		—	—			—		
31		—		—	—				—			—		—		—		—		—	—					—
37	—		—		—	—							—	—		—	—			—	—	—		—		
41	—	—		—						—		—	—	—	—			—	—			—		—		
43						—	—	—		—		—		—	—	—	—	—		—			—	—		—
47		—	—		—			—					—			—	—	—	—		—	—	—	—	—	—
53	—				—	—	—	—			—		—		—	—	—	—							—	—
59			—	—	—			—	—		—			—			—	—			—		—			
61	—		—	—			—		—					—		—			—			—		—		—
67								—	—	—	—		—			—		—		—	—	—		—	—	
71		—	—	—					—		—		—		—						—	—	—	—	—	
73	—	—	—						—	—			—	—					—	—	—	—	—		—	—
79		—		—		—	—		—	—		—								—		—	—	—	—	—
83			—		—	—		—		—	—	—	—	—				—	—					—		
89	—	—		—		—		—								—	—			—	—	—	—		—	—
97	—	—	—			—						—			—	—	—		—			—	—		—	—

Tabla III. (artículo 316)

3	(0)...3; (1)...6
7	(0)...142857
9	(0)...1; (1)...2; (2)...4; (3)...8; (4)...7; (5)...5
11	(0)...09; (1)...18; (2)...36; (3)...72; (4)...45
13	(0)...076923; (1)...461538
17	(0)...0588235294 117647
19	(0)...0526315789 47368421
23	(0)...0434782608 6956521739 13
27	(0)...037; (1)...074; (2)...148; (3)...296; (4)...592; (5)...185
29	(0)...0344827586 2068965517 24137931
31	(0)...0322580645 16129; (1)...5483870967 74193
37	(0)...027; (1)...135; (2)...675; (3)...378; (4)...891; (5)...459
	(6)...297; (7)...486; (8)...432; (9)...162; (10)...810; (11)...054
41	(0)...02439; (1)...14634; (2)...87804; (3)...26829; (4)...60975; (5)...65853; (6)...95121; (7)...70731
43	(0)...0232558139 5348837209 3; (1)...6511627906 9767441860 4
47	(0)...0212765957 4468085106 3829787234 0425531914 893617
49	(0)...0204081632 6530612244 8979591836 7346938775 51
53	(0)...0188679245 283; (1)...4905660377 358; (2)...7547169811 320; (3)...6226415094 339
59	(0)...0169491525 4237288135 5932203389 8305084745 7627118644 06779661
61	(0)...0163934426 2295081967 2131147540 9836065573 7704918032 7868852459
67	(0)...0149253731 3432835820 8955223880 597; (1)...1791044776 1194029850 7462686567 164
71	(0)...0140845070 4225352112 6760563380 28169; (1)...8732394366 1971830985 9154929577 46478
73	(0)...01369863; (1)...06849315; (2)...34246575; (3)...71232876; (4)...56164383
	(5)...80821917; (6)...04109589; (7)...20547945; (8)...02739726
79	(0)...0126582278 481; (1)...3670886075 949; (2)...6455696202 531
	(3)...7215189873 417; (4)...9240506329 113; (5)...7974683544 303
81	(0)...012345679; (1)...135802469; (2)...493827160; (3)...432098765; (4)...753086419; (5)...283950617
83	(0)...0120481927 7108433734 9397590361 4457831325 3
	(1)...6024096385 5421686746 9879518072 2891566265 0
89	(0)...0112359550 5617977528 0898876404 4943820224 7191
	(1)...3370786516 8539325842 6966292134 8314606741 5730
97	(0)...0103092783 5051546391 7525773195 8762886597 9381443298 9690721649 4845360824 7422680412
	3711340206 185567

CONTENIDOS.

DEDICACION. . . . . p. 1

PREFACIO. . . . . p. 3

SECCION PRIMERA. De la congruencia de los números en general . . . . . p. 7

Números congruentes, módulos, residuos y no residuos, art. 1
Residuos mínimos, art. 4
Proposiciones elementales sobre congruencias, art. 5
Algunas aplicaciones, art. 12

SECCION SEGUNDA. Sobre las congruencias del primer grado . . . . . p. 13

Teoremas preparatorios sobre los números primos, factores, etc., art. 13
La resolución de las congruencias del primer grado, art. 26
Acerca de la búsqueda de un número congruente a un número dado según un módulo dado, art. 32
Congruencias lineales con varias incógnitas, art. 37
Varios teoremas, art. 38

SECCION TERCERA. Sobre residuos de las potencias . . . . . p. 38

Los residuos de los términos de una progresión geométrica que comienza desde la unidad constituyen una serie periódica, art. 45
Se consideran primero los módulos que son números primos.
El número de términos en el período es un divisor de $p-1$ si el módulo $= p$, art. 49

El teorema de Fermat, art. 50

Cuantos números corresponden a un período, en el cual el número de términos es un divisor dado del número $p-1$, art. 52

Raíces primitivas, bases e índices, art. 57

Algoritmos de los índices, art. 58

Sobre las raíces de la congruencia $x^n \equiv A$, art. 60

La conexión entre los indices en sistemas diferentes, art. 69

Bases adaptadas para usos especiales, art. 72

Método para la determinación de las raíces primitivas, art. 73

Varios teoremas sobre los períodos y las raíces primitivas, art. 75

(El teorema de Wilson, art. 76)

Sobre los módulos que son potencias de números primos, art. 82

Módulos que son potencias de 2, art. 90

Módulos compuestos de varios primos, art. 92

Seccion Cuarta. Sobre las congruencias de segundo grado . . . . . p. 73

Residuos y no residuos cuadráticos, art. 94

Cuando el módulo es un número primo, el número de residuos menores que el módulo es igual al número de no residuos menores, art. 96

La cuestión de si un número compuesto es un residuo o un no residuo de un número primo dado depende de la naturaleza de los factores, art. 98

Sobre los módulos que son números compuestos, art. 100

Criterio general sobre si un número dado es un residuo o un no residuo de un número primo dado, art. 106

Investigaciones sobre los números primos cuyos residuos o no residuos sean números dados, art. 107

Residuo -1, art. 108

Residuos $+2$ y -2, art. 112

Residuos $+3$ y -3, art. 117

Residuos $+5$ y -5, art. 121

Sobre ± 7, art. 124

Preparación para la investigación general, art. 125

Por inducción se apoya un teorema general (fundamental), y se deducen algunas conclusiones de él, art. 130
Demostración rigurosa del teorema fundamental, art. 135
Método análogo para la demostración del teorema del art. 114, art. 145
La resolución del problema general, art. 146
Sobre las formas lineales que contienen todos los números primos de los cuales un número dado cualquiera es un residuo o no residuo, art. 147
Sobre los trabajos de otros acerca de estas investigaciones, art. 151
Sobre las congruencias no puras del segundo grado, art. 152

SECCION QUINTA. Sobre las formas y las ecuaciones indeterminadas de segundo grado . . . . . p. 121

Propósito de la investigación: definición y notación de las formas, art. 153
Representación de los números; el determinante, art. 154
Los valores de la expresión $\sqrt{b^2 - ac}$ (mod. M) a los cuales pertenece la representación del número M por la forma (a, b, c), art. 155
Una forma que implica otra o contenida en ella; la transformación propia e impropia, art. 157
La equivalencia propia e impropia, art. 158
Formas opuestas, art. 159
Formas contiguas, art. 160
Divisores comunes de los coeficientes de las formas, art. 161
El nexo de todas las transformaciones semejantes de una forma dada en otra forma, art. 162
Formas ambiguas, art. 163
Teorema sobre el caso en que una forma está contenida en otra al mismo tiempo propia e impropiamente, art. 164
Generalidades sobre las representaciones de los números por las formas y su nexo con las transformaciones, art. 166
Sobre las formas de un determinante negativo, art. 171
Aplicaciones especiales a la descomposición de los números en dos cuadrados, en un simple y un doble cuadrado, en un simple y un triple cuadrado, art. 182
Sobre las formas de un determinante positivo no cuadrado, art. 183

Formas de determinante cuadrado, art. 206
Formas contenidas en otras a las cuales no son equivalentes, art. 213
Formas con determinante 0, art. 215
Solución general de toda ecuación indeterminada de segundo grado con dos incógnitas, art. 216
Anotaciones históricas, art. 222

Investigaciones ulteriores sobre las formas

Distribución de formas de un determinante dado en clases, art. 223
Distribución de clases en órdenes, art. 226
La partición de órdenes en géneros, art. 228
Sobre la composición de formas, art. 234
Composición de órdenes, art. 245
Composición de géneros, art. 246
Composición de clases, art. 249
Para un determinante dado existe el mismo número de clases en cada género del mismo orden, art. 252
Se comparan el número de clases contenidas en géneros individuales de órdenes distintos, art. 253
Sobre el número de clases ambiguas, art. 257
La mitad de todos los caracteres asignables para un determinante dado no puede pertenecer a un género propiamente primitivo (positivo para un determinante negativo), art. 261
Una segunda demostración del teorema fundamental y de los demás teoremas acerca de los residuos -1, $+2$, -2, art. 262
Se determina más exactamente la mitad de los caracteres que no pueden corresponder a ningún género, art. 263
Un método especial para descomponer primos en dos cuadrados, art. 265

Una digresión conteniendo un estudio de formas ternarias, art. 266

Algunas aplicaciones a la teoría de las formas binarias.
Para encontrar una forma cuya duplicación produce una forma binaria dada del género principal, art. 286

Todos los caracteres, salvo aquéllos mostrados como imposibles en art. 263 y 264, petenecen a algún género, art. 287

La teoría de la descomposición de números y formas binarias en tres cuadrados, art. 288

Demostración de los teoremas de Fermat: todo entero puede descomponerse en tres números triangulares o cuatro cuadrados, art. 293

Solución de la ecuación $ax^2 + by^2 + cz^2 = 0$, art. 294

Sobre el método con el cual Legendre trató de demostrar su teorema fundamental, art. 296

Representaciones de cero por formas ternarias cualesquiera, art. 299

Solución general de ecuaciones indeterminadas de segundo grado en dos variables por racionales, art. 300

Del número promedio de géneros, art. 301

Del número promedio de clases, art. 302

Algoritmo singular para clases propiamente primitivas; determinantes regulares e irregulares, etc., art. 305

Seccion Sexta. Aplicaciones varias de las investigaciones precedentes. . p. 387

De la descomposición de fracciones en otras más simples, art. 309

La conversión de fracciones comunes en decimales, art. 312

Solución de la congruencia $x^2 \equiv A$ por el método de exclusión, art. 319

Solución de la ecuación indeterminada $mx^2+ny^2 = A$ por exclusiones, art. 323

Otro método de resolver la congruencia $x^2 \equiv A$ para el caso en que A es negativo, art. 327

Dos métodos para distinguir números compuestos de números primos y para determinar sus factores, art. 329

Seccion Setima. Ecuaciones que definen secciones de un círculo. . . . p. 419

La discusión se reduce al caso más simple, donde el número de partes en las cuales se corta el círculo es un número primo, art. 336

Ecuaciones para funciones trigonométricas de arcos que son una parte o partes de la circunferencia completa, reducción de las funciones trigonométricas a las raíces de la ecuación $x^n - 1 = 0$, art. 337

Teoría de las raíces de la ecuación $x^n - 1 = 0$ *(donde n es primo).*
Omitiendo la raíz 1, las restantes (Ω) están en la ecuación
$X = x^{n-1} + x^{n-2}$+etc.$+x + 1 = 0$. La función X no se puede descomponer en factores con coeficientes racionales, art. 341
Declaración del propósito de las investigaciones siguientes, art. 342
Todas las raíces de Ω se distribuyen en ciertas clases (períodos), art. 343
Varios teoremas concernientes a estos períodos, art. 344
La solución de la ecuación $X = 0$ según se desarrolla de la investigación precedente, art. 352
Ejemplo para $n = 19$ donde la operación se reduce a resolver dos ecuaciones cúbicas y una cuadrática, art. 353
Ejemplo para $n = 17$ donde la operación se reduce a resolver cuatro ecuaciones cuadráticas, art. 354
Investigaciones adicionales sobre los períodos de raíces.
Sumas con un número par de términos son cantidades reales, art. 355
De la ecuación que define la distribución de las raíces Ω en dos períodos, art. 356
Demostración de un teorema mencionado en Sección IV, art. 357
De la ecuación que distribuye las raíces Ω en tres períodos, art. 358
Reducción a ecuaciones puras de las ecuaciones que dan las raíces Ω, art. 359
Aplicación de lo anterior a funciones trigonométricas.
Método para encontrar los ángulos de raíces particulares en Ω, art. 361
Se derivan tangentes, cotangentes, secantes y cosecantes a partir de senos y cosenos sin división, art. 362
Método de reducir sucesivamente las ecuaciones para funciones trigonométricas, art. 363
Secciones del círculo que pueden realizarse por ecuaciones cuadráticas o sea por construcciones geométricas, art. 365

APENDICE. . . . . p. 473

TABLAS. . . . . p. 475

APENDICE.

NOTAS MANUSCRITAS DE GAUSS.

Al art. 40. *Si hay un tercer número C, sea λ' el máximo común divisor de los números λ y C, y determínense números k y γ, tales que $k\lambda + \gamma C = \lambda'$, entonces $k\alpha A + k\beta B + \gamma C = \lambda'$. Es evidente que también λ' es un divisor común de los números A, B y C, y, de hecho, el máximo, puesto que si hubiera otro mayor $= \theta$, resultaría*

$$k\alpha \cdot \frac{A}{\theta} + k\beta \cdot \frac{B}{\theta} + \gamma \cdot \frac{C}{\theta} = \frac{\lambda'}{\theta} \quad \textit{entero}, \quad \textit{Q.E.A.}$$

Así se obtiene lo que íbamos a mostrar al poner $k\alpha = a$, $k\beta = b$, $\gamma = c$ y $\lambda' = \mu$.

Al art. 114. *Una demostración más elegante se hace como sigue:*

$$(a^{3n} - a^n)^2 = 2 + (a^{4n} + 1)(a^{2n} - 2)$$
$$(a^{3n} + a^n)^2 = -2 + (a^{4n} + 1)(a^{2n} + 2)$$

y así $\sqrt{2} \equiv \pm(a^{3n} - a^n)$ *y* $\sqrt{-2} \equiv \pm(a^{3n} + a^n) \pmod{8n+1}$.

Al art. 256 VI. Indicamos 16 determinantes positivos de la forma $8n + 5$ para los cuales el número de clases propiamente primitivas es tres veces mayor que el número de clases impropiamente primitivas, a saber $37, \ldots, 573$. A éstos se agregan *677, 701, 709, 757, 781, 813, 829, 877, 885, 901, 909, 925, 933, 973, 997, resultando 31 de los 125.*

Al art. 301. De esta manera la suma del número de géneros para los determinantes -1 a -100 resulta ser $= 234,4$, mientras que su valor real es 233. — — *De –1 a –3000, la tabla da 11166, la fórmula 11167,9.*

Al art. 366. *Si todos los números* $2^{2^m}+1$ *fueran primos, entonces una aproximación suficientemente precisa para el número (N) de enteros de este tipo menores que un número M dado sería* $\frac{1}{2}(\frac{\log M}{\log 2})^2$.

Al art. 42. El teorema concerniente a los divisores de una función algebraica racional entera con coeficientes enteros. — — *22 de julio de 1797.*

Al art. 130. Después de haber demostrado rigurosamente que cada número primo de la forma $4n+1$, tomado positivo o negativamente, es un no residuo de algún número primo menor que él mismo. — — *Descubrimos esta prueba el 8 de abril de 1796.*

Al art. 131. *Descubrimos el teorema fundamental por inducción en marzo de 1795.*

Encontramos nuestra primera prueba, aquélla contenida en esta sección, en abril de 1796.

Al art. 133. Iniciamos ahora una investigación más general. Consideraremos dos números impares cualesquiera P y Q, primos entre sí, provistos de signos cualesquiera. — — *29 de abril de 1796.*

Al art. 145. Además, los teoremas pertenecientes a los residuos $+2$ y -2 entonces deberían suponerse; pero como nuestra demostración está completa sin usar estos teoremas, obtenemos de esto un método nuevo para demostrarlos. — — *4 de febrero de 1797.*

Al encabezamiento de la Sección V: Sobre las formas y las ecuaciones indeterminadas de segundo grado. — — *De aquí adelante, 22 de junio de 1796.*

Al art. 234. . . . pasaremos a otro tema muy importante, la composición de formas. — — *Estas disquisiciones fueron iniciadas en el otoño de 1798.*

Al art. 262. A partir de este principio, podemos desarrollar un nuevo método, no solamente para el teorema fundamental, sino también para demostrar los otros teoremas de la sección previa que tengan que ver con los residuos -1, $+2$, -2. — — *Los principios de este método fueron primero descubiertos el 27 de julio de 1796, pero fue refinado y reducido a su forma presente en la primavera de 1800.*

Al art. 266. . . . pero hay muchas verdades bellas concernientes a estas formas cuya fuente real se indaga en la teoría de formas ternarias de segundo grado. Haremos, por tanto, una breve digresión dentro de esta teoría. — — *14 de febrero de 1799.*

Al art. 272. Primero mostraremos cómo cada forma ternaria puede ser reducida a una forma más simple y luego mostraremos que el número de las formas más simples (que resulta de tales reducciones) es finito para un determinante dado. — — *13 de febrero de 1800.*

Al art. 287 III. De manera similar se prueba que aquellos caracteres en un orden impropiamente primitivo, que según los métodos de los artículos 264 II, III resultan ser los únicos posibles, son realmente del todo posibles, independientemente de si pertenecen a P o a Q. Creemos que estos teoremas, etc. — — *Se probaron por primera vez en el mes de abril de 1798.*

Al art. 302. El número promedio de clases, sin embargo, (no hace falta una definición) aumenta de manera muy regular. — — *Una primera idea en el comienzo de 1799.*

Al art. 306 X. Finalmente hacemos notar que, puesto que todas las propiedades consideradas en este artículo y el anterior dependen especialmente del número n, el cual juega un papel similar al de $p-1$ en la Sección III, este número merece atención cuidadosa. Es muy deseable por lo tanto determinar la relación general entre este número y el determinante al cual pertenece. — — *Todo lo que queríamos resultó tan bueno que no dejó nada que desear. 30 de noviembre– 3 de diciembre de 1800.*

Al art. 365. *Descubrimos que un círculo es geométricamente divisible en 17 partes el 30 de marzo de 1796.*

INDICE DE TERMINOS

carácter
completo, 238.
de una forma, 237.
clase
ambigua, 230.
compuesta, 277.
de formas, 228.
derivada de una clase primitiva, 232.
duplicación de una, 278.
impropiamente primitiva, 232.
negativa, 231.
opuesta, 230.
positiva, 231.
primitiva, 232.
principal, 239.
propiamente primitiva, 232.
congruencia, 18.
algebraica, 18.
resoluble, 18.
resuelta, 18.
trascendental, 18.
determinante
de una forma, 123, 306.
irregular, 380.
regular, 380.
exponente de irregularidad, 381.
forma
adjunta, 306.
ambigua, 137.
asociada, 173.
binaria, ternaria, etc., 304.
compuesta de dos formas, 247.
tomada directamente, 250.
tomada inversamente, 250.
forma (*cont.*)
compuesta directamente, 250.
compuesta inversamente, 250.
compuesta por tres formas, 265.
compuesta por varias formas, 265.
contenida
en otra, 125.
impropiamente, 126.
propiamente, 126.
contigua, 129.
a la primera parte, 129.
a la última parte, 129.
de los divisores, 113.
de los no divisores, 113.
de segundo grado, 121.
de segundo, tercero, cuarto grado, etc., 304.
definida, 310.
derivada, 231.
equivalente, 126.
impropiamente, 127.
propiamente, 127.
impropiamente primitiva (impropia), 232.
indefinida, 310.
negativa, 231, 310.
opuesta, 129.
positiva, 231, 310.
primitiva, 231.
principal, 239.
propiamente primitiva (propia), 232.
que implica otra, 125.
que se puede descomponer en formas, 270.

forma (*cont.*)
reducida, 150, 167, 205.
representante de una clase, 228.
transformable en ff', 247.
género, 238.
compuesto, 276.
principal, 240.
índice, 47.
magnitud del período de una fracción, 391.
mantisa de una fracción, 389.
módulo, 7.
no residuo, 7.
número
asociado, 61.
característico de una forma, 243.
congruente a otro según un módulo, 7.
excluyente, 396, 399.
incongruente a otro según un módulo, 7.
perteneciente a un exponente, 43.
período, 171.
asociado, 174.
de una clase, 379.
de una fracción, 391.
(f, λ), 428.
similar, 428.
permutación semejante, 33.
raíz
primitiva, 46, 69.
recíproca, 423.
representación
adjunta, 325.
del mismo orden, 233.
de una forma perteneciente a un divisor cuadrado, 336.
de un número por una forma, 122.
impropia, 326.
perteneciente a un valor, 331.
propia, 326.
residuo, 7.
absolutamente mínimo, 8.
asociado, 83.
cuadrático, 74, 241.
mínimo, 8.
transformación
desemejante, 126.
impropia, 126.
propia, 126.
semejante, 126.
triplicación de una clase, 278.
valor
de la expresión $\sqrt{ax^2 + 2bxy + cy^2}$, 241.
diferente, 243.
equivalente, 243.
opuesto, 331.